MASTER'S THESIS

Information Security Awareness of bank employees: how differences between headquarter and branch employees affect ISA program design

Takens, N.D.

Award date:
2020

Information Security Awareness of bank employees: how differences between headquarter and branch employees affect ISA program design

Opleiding:	Open Universiteit, faculteit Bètawetenschappen Masteropleiding Business Process Management & IT
Degree programme:	Open University of the Netherlands, Faculty of Science Business Process Management & IT Master's programme
Course:	IM0602 BPMIT Graduation Assignment Preparation IM9806 Business Process Management and IT Graduation Assignment
Student:	N.D. Takens
Identification number:	
Date:	4 June 2020
Thesis supervisor	Prof. Dr. A. Bijlsma
Second reader	Dr. L.W. Rutledge
Third assessor	Not applicable
Version number:	1.0
Status:	Final version

Abstract

It is commonly acknowledged that human behavior is a factor that should not be underestimated when it comes to Information Security (IS). Information Security Awareness (ISA) programs are set up as a preventive measure, but breaches remain to occur. In order to develop tailored ISA programs that fit user's needs, insight is necessary. Banks hold valuable personal and financial information which makes them a target for cyber criminals and therefore, the aim of our descriptive research was to gain insight in differences between headquarter and branch employees in the banking industry. By applying the Human Aspects of Information Security Questionnaire (HAIS-Q), we were able to show that differences are present between the two groups, especially in the area's password management, email use and social media use. This suggests that tailoring programs could benefit ISA of these bank employees. Based on our results, we presented propositions that could be examined in future research within banking, but also other sectors belonging to the financial industry.

Key terms

Information security awareness, information security awareness programs, Information security policy compliance, banking, employee groups

Summary

The way we are communicating these days has changed drastically in the last decades. All aspects of our lives are integrated with digital solutions. We use our computers and smart devices for communication around the world, ordering groceries online and managing our finances in our banking applications. Obviously, this digitalization is bringing a lot of benefits, however, it also involves risks regarding the security of our information. A high level of information security is important to such an extent, that a lack of it could eventually even lead to social disruption and stagnating economic growth. Despite the possibilities to decrease security risks through technical solutions, human behavior is an aspect that cannot be overlooked. Several reports confirm that human behavior is a vulnerability, which therefore encourages organizations to set up information security awareness (ISA) programs. ISA is a preventive measure with regards to security breaches that are caused by human behavior but in order to be effective, programs should be tailored to the user's needs.

Banks are key players in our financial infrastructure, and they are holding a lot of valuable client- and financial information. At the same time, this information is considered to be most valuable to cyber criminals. This stretches the need for adequate information security measures, including those related to human behavior. Only limited research has been carried out regarding ISA of bank employees, while authors of prior studies have recommended to gain insight in different user perspectives. The importance of banks and the information they hold, in combination with the need for ISA programs that are fit to the user's needs, were the primary reasons for us to conduct research in this context. Our cross-sectional, embedded single case study took place at one of the largest banks in the Netherlands. As a result of our descriptive research, we were able to formulate several propositions that could be further examined in future research.

Within the banking industry there are two major employee groups; headquarter employees and branch employees. However, both groups are different to a large extent. Headquarter employees are working mainly with internal parties, in jobs related to HR, Marketing, IT, (Product) Management et cetera. Branch employees on the other hand, are having frequent contact with external parties such as clients or client representatives (e.g. accountants, financial advisors). These differences in daily work mean that both groups face different information security (IS) risks, which implies that they have different needs related to ISA programs. In order to map the differences between both groups, we have measured both groups ISA on five difference focus areas by using the Human Aspects of Information Security Questionnaire (HAIS-Q). The original instrument consists of seven focus areas, however, after conducting a semi-structured focus group interview with two Information Security Specialists we decided to apply a reduced version since this matched best with the case organization. In our paper, we refer to this reduced version of the HAIS-Q as the R-HAIS-Q, which included the focus areas password management, email use, social media use, mobile devices and incident reporting. These focus areas included statements based on the knowledge, attitude and behavior (KAB) model, where answers could be provided on a 5-point Likert scale.

The results of the R-HAIS-Q have provided us with interesting observations. Within the 'mobile devices' and 'incident reporting' focus areas no significant differences could be found. However, within the remaining three areas, several significant differences between both groups were detected.

Firstly, within the password management focus area, we have found that headquarter employees are showing significantly better attitude towards the use of strong passwords. At the same time, no differences are observed in the related knowledge and behavior statements. This suggests that branch

employees know about policy regarding the use of strong passwords and also bring this knowledge into practice, but that they are less intrinsically motivated to do so.

Secondly, our research provided relevant insights related to handling emails from unknown senders. Branch employees are showing significantly better knowledge of policy and procedures regarding clicking on links and opening attachments. Despite their knowledge, their self-reported behavior shows that they do click on links in these (possibly phishing) emails. Headquarter employees are showing that they do not necessarily need knowledge regarding this topic in order to practice compliant behavior. Presumably, this is easier for them to do so, since they are less likely to have external contact. It is assumable that branch users are having more email contact with unknown external parties, which accordingly might lead to clicking on links in those emails. However, this behavior is not reflected with regards to opening attachments in emails from unknown senders. A limitation of this research is that we could not validate these assumptions, since we are not aware of the extent to which the respondents have email contact with unknown parties. Therefore, when testing our propositions, we recommend dedicating special attention to this aspect.

Thirdly, headquarter employees are showing significantly better awareness on social media use. Both groups are not differing from each other when it comes to knowledge of policy regarding social media privacy settings. However, headquarter employees show significantly better attitude and self-reported behavior than branch employees. Prior research has indicated that increasing knowledge leads to better attitude and behavior. We propose that doing so will have positive impact on branch employees ISA. For headquarter employees on the other hand, we postulate that they are likely not to need knowledge in order to show compliant attitude and behavior. Another subject related to social media use is the consideration of consequences. Branch users have less knowledge about possible consequences for their employment when posting online, but this is not reflected in their self-reported behavior (where both of them have nearly perfect scores). This suggests that the employee groups don't need to know the possible consequences of posting online, since they will do the right thing anyway.

Looking at the size of our samples and the applied sampling technique (self-selection sampling), this implies that it is unlikely that our sample is representative for full populations. Also, it would've been beneficial for the reliability of our study to investigate when the respondents of the questionnaire had their last ISA interventions (and what it entailed). However, taking these limitations in consideration, our descriptive research has provided insight in potential differences between headquarter and branch employees, which enabled us to formulate several propositions which could be further examined in future research.

Contents

1. Introduction

1.1. Background

Without doubt, we all can recognize that there has been a significant change in how we handle and transport information these days. Where our grandparents, in the 20th century, were used to sending hand-written letters, the current generations use digital solutions to transfer their messages and exchange information. According to Davison & Chen (1995), it all started in the United States of America in the 1960s, when the Department of Defense found that the communication system that was used back then was too fragile. For several reasons, there was a high risk that in certain circumstances important messages would not reach their destination. This food for thought for researchers, together with the development of the necessary hardware, formed the basis of the internet as we know it.

Nowadays, we cannot imagine living without internet and all the related solutions. It has embedded in every aspect of our daily lives. We can order our groceries online, manage our finances through online banking and we can have a quick, high resolution video call through our smart phones with people all around the world. The digital revolution is on-going and information technology (IT) is continually integrated in organizations. Despite the benefits that come with those technologies, it does not take away the risks of possible information security breaches (Sohrabi Safa, Von Solms, & Furnell, 2016). According to a recent report on cyber security in The Netherlands (Nctv, 2019), there currently is high dependency on digitalized processes and systems which emphasizes the need of adequate digital safety. A lack of digital safety may ultimately even result in stagnating economic growth and can initiate social disruption. This underlines the need for research on information security (IS) management.

There are multiple technological solutions to increase information security (e.g. firewalls, anti-virus software), but reports are showing that human behavior remains a vulnerability that should not be overlooked (Ernst & Young Global Limited, 2019; Nctv, 2019). A preventive measure to the problem of information security breaches caused by humans can be found in increasing information security awareness (ISA) amongst employees. Therefore, ISA programs are set up by organizations to increase awareness regarding how to handle in certain IS situations, with the ultimate goal to comply to the applicable information security policies (Bauer, Bernroider, & Chudzikowski, 2017; Bawazir, Mahmud, Molok, & Ibrahim, 2016).

In this research, we are taking a deep dive into ISA, with a focus on differences between headquarter and branch employees, in a banking organization in The Netherlands. This paper starts off with the problem statement, research questions, motivation and relevance, as well as a high-level research approach. The theoretical framework gives insight in the current body of knowledge regarding this subject. Our empirical study opened with a focus group interview in order to come to a Human Aspects of Information Security Questionnaire (HAIS-Q) which suits our case study (organization). The results are presented in Chapter 4 and our paper is finalized with a discussion, conclusions and recommendations in Chapter 5.

1.2. Problem statement

The banking industry is an industry which has to deal with continually changing legislation and an increase of competition, e.g. due to a growing number of FinTech firms (Li, Spigt, & Swinkels, 2017). In order to keep up with this continually changing environment it is deemed necessary to remain innovative regarding their used technologies (Goldstein, Chernobai, & Benaroch, 2011). While introducing new technologies, it remains important to take the necessary measures to keep the processed information secure, thus to comply to applicable legislation. It is obvious that banks hold a lot of customer and financial information and according to Ernst & Young Global Limited (2019), this data is the most valuable information to cyber criminals. This underlines the need for the banking industry to do its utmost to guarantee their IS. A general issue regarding the security of information, is the finding that 34% of organizations see unaware and/or careless employees as the biggest vulnerability. On top of that, a report of the Nctv (2019), confirms that in 2018 over 50% of the reported data breaches in The Netherlands were found to be the result of errors caused by humans. According to several authors, the results of their research have shown positive effects of ISA on ISP compliance (Bauer & Bernroider, 2017; Bauer et al., 2017), but nevertheless, figures are showing shocking percentages on the involvement of humans in relation to the total number of data breaches.

1.3. Research objective and questions

ISA programs are an important means to inform and educate employees of an organization about IS and related risks. Because human error has a large part in the total amount of data breaches, it is likely that ISP compliance increases when a higher level of ISA is reached amongst employees. Banks hold valuable client- and financial information, which makes them an interesting target to hackers.

In order to state what we want to achieve with this research, we formulated a research aim (Saunders, Lewis, & Thornhill, 2016). The aim of this research is to provide detailed insight in the differences on ISA between headquarter and branch employees, which are two specific, distinct user groups, with different roles and responsibilities. The results evolving from this research gives both researchers and practitioners the ability to further research and develop ISA programs which may increase ISA within organizations.

The problem statement is formulated as follows:

What aspects of headquarter and branch employees in the banking industry influence the design and effectiveness of an ISA program? And how?

The problem statement has been subdivided in a number of research questions.

Part 1: Theoretical foundation

1.a How is an ISP formed and what is ISP compliance?
1.b What is ISA and how can the design of an ISA program contribute to increasing ISA?
1.c How can users' ISA be measured?

Part 2: Application of the research framework

2.a What are the differences on ISA between headquarter and branch employees?
2.b To what extent can the obtained insights contribute to the design of ISA programs?

Part 1 will be answered through a critical literature review. Part 2 is the empirical part of this research.

1.4. Motivation/relevance

There are many sources that confirm the social relevance of research contributing to IS. In their report, the World Economic Forum (2018) state that both cyber-attacks and data fraud & theft are amongst the top 5 global risks in terms of likelihood. In addition, according to Ernst & Young Global Limited (2019), 6.4 billion fake emails are being sent around the globe on a daily basis and the average cost of one single data breach in 2017 was $3.62 million. Despite efforts of raising ISA through preventive ISA programs, human behavior remains to have a large part in data breaches which questions the effectivity of these programs. If no research will be conducted on ISA of users, it is doubtful that the amount of human errors will decrease.

1.5. Main lines of approach

Our research took place in the banking industry, since banks hold a lot of client and financial information which could be precious to malicious people. By giving insight in ISA of headquarter and branch employees within a banking organization, our research contributes to the existing body of knowledge regarding the design and improvement of ISA programs. Our results could help banks, and possibly other organizations in e.g. the financial services industry, in educating employees regarding IS risks and thus improving ISA. The main lines of approach for this research are outlined in figure 1.

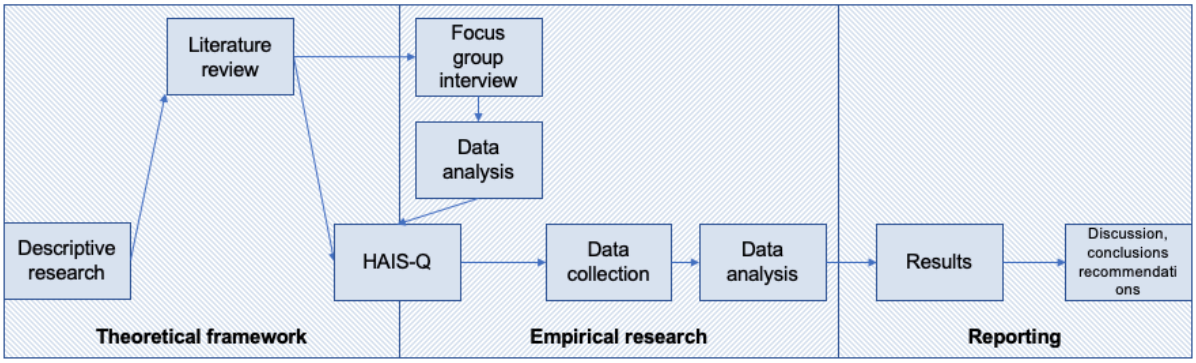

Figure 1: Main lines of approach

2. Theoretical framework

2.1. Research approach and implementation

The theoretical framework consists of the literature research approach and implementation, the results, conclusions and objectives of the follow-up research. A full overview of the approach, steps taken, and results can be found in appendix 1.

2.2. Results and conclusions

In the paragraphs below, the theoretical framework can be found which includes the answers to the research questions (1.a, 1.b and 1.c) with arguments supporting them. Also, information is shared with regards to the research field, language and definitions that are used.

2.2.1. How is an ISP formed and what is ISP compliance? (1.a)

Information security and cyber security – First, we found out that information security and cyber security are two terms that are used interchangeably. Although cyber security and information security show similarities, there is a slight difference. According to Von Solms & Van Niekerk (2013), cyber security goes beyond information security. Information security is basically defined in terms of availability, integrity and confidentiality and is about protection of information from threats and vulnerabilities. Cyber security is about more than protecting information, and includes the protection of people, societal values and national infrastructure as well. Von Solms & Van Niekerk (2013) explain further that basically, in information security, information is the asset that should be protected where information and communication technology (ICT) actually is the vulnerability. Both components are interrelated when it comes to information security and thus, cannot be viewed separately (Von Solms & Van Niekerk, 2013).

Information Security Policy – The relation of information with ICT fits well with applicable banking regulations. Luthy & Forcht (2006) explain that the Basel Committee on Banking Supervision (BIS) acknowledged that risks may evolve from information management systems. As a response, BIS formed requirements regarding risks related to information management systems in their Basel II Accord, where banks have to comply to. An ISP is both a security control and guideline for users regarding information management (Höne & Eloff, 2002). It may consist of a wide variety of business and security related topics but should always include legal and regulatory requirements in order to protect information (Da Veiga & Martins, 2015). Höne & Eloff (2002) substantiate that international standards are primarily used in developing an ISP, despite the fact that those standards mostly are not very detailed in their explanations. With regards to the development of an ISP, it is important that the final guidelines and policy documentation are meeting the needs of the organization and its culture. Several general elements are essential to be part of it as well, such as background information, explanation of the purpose of the document, a definition of IS, IS principles and roles & responsibilities. On top of that, it should be easy to read and be fit to the end-user (Höne & Eloff, 2002). Meeting those requirements and having the ISP available to employees on both traditional and digital channels, contributes to the awareness of information security issues (Haeussinger & Kranz, 2013).

ISP compliance and noncompliance – Unfortunately, we haven't found a singular definition of ISP compliance. Therefore, we follow Moody, Siponen, & Pahnila (2018) who refer to user's ISP compliance as *"an employee's compliance with information security policies, procedures or guidelines"* (p. 286). Violating an ISP can obviously occur intentionally, but also unintentionally. User's unintentional noncompliance with ISP's involves actions such as e.g. careless behavior, but an important risk here is

that this can be exploited by other malicious individuals who want to make use of the opportunity to gain access to a company's information (Guo, Yuan, Archer, & Connelly, 2011). Furthermore, abusing a company's computer with actions such as visiting unsafe web content or downloading valuable, confidential company data are causes of noncompliant behavior (Siponen & Vance, 2010). Factors that influence the intention to comply are found in e.g. neutralization techniques such as denial of responsibility, defense of necessity or denial of injury (Siponen & Vance, 2010), but noncompliance can also be related to ISP-related personal norms (Yazdanmehr & Wang, 2016). To have employees complying to ISP's, the benefits of doing this should be clear to them (Han, Kim, & Kim, 2017). Another successful way to prevent user's in ISP noncompliance is ISA (Haeussinger & Kranz, 2013) but additional research, especially with a focus on individuals and their perceptions, is recommended (Bauer et al., 2017).

Conclusion – ISP noncompliance, thus violation of ISP's, procedures or guidelines, can occur both intentionally and unintentionally. In order to lower the risks related to IS, an ISP should be formed which consists of a.o. legal and regulatory requirements that meet the needs of the organization. On top of that, the ISP should be fit to the end-user, easy to read, and it should emphasize the benefits of compliance.

2.2.2. What is ISA and how can the design of an ISA program contribute to increasing ISA? (1.b)

Information Security Awareness – Several definitions of ISA are being used by researchers. According to Siponen (2000), ISA can be referred to as *"a state where users in an organization are aware of their security mission"* (p. 31), but also a more extensive definition is being used. Bulgurcu, Cavusoglu, & Benbasat (2010) are presenting a definition of ISP awareness, which is *"an employee's knowledge and understanding of the requirements prescribed in the organization's ISP and the aims of those requirements"* (p. 532). In their substantiation, they explain that there is a distinction between general ISA (which refers to the overall knowledge of IS risks) and ISP awareness (which refers specifically to awareness regarding policies). Therefore, we are following their determination in which ISA is formed by both ISP awareness and general ISA, in particular because an ISP is considered a valuable control in the area of an organization's IS (Höne & Eloff, 2002).

ISA programs – Plausibly, ISP's are created for an organization and its employees to comply to, but in order to increase ISP compliance, ISA is key (Haeussinger & Kranz, 2013). In their research, Sohrabi Safa et al. (2016) argue that ISP's contribute to the prevention of security breaches by employees, but their findings confirm that employees that are committed to an organization are more likely to comply to ISP's than the less committed. This is in line with Wiley et al. (2020), who argue that a higher level of organizational culture has a positive influence on ISA. However, they explicate that security culture plays a substantial role in this relationship and therefore it should have high priority in efforts regarding increasing ISA. Focusing on security culture can be done by guiding employees towards acceptable and compliant behavior in protecting information assets (Da Veiga & Martins, 2015). This includes, amongst others, sharing IS knowledge, but also adequate training can be a successful means with regards to decreasing information security breaches (Haeussinger & Kranz, 2013; Sohrabi Safa et al., 2016). In contrast, Bauer & Bernroider (2017) state that knowledge sharing between employees is irrelevant, but they do find agreement upon using posters, leaflets and other internal communication as successful means for increasing ISA. It should be part of an internal and external channel approach, where making use of e.g. e-learnings (internal) and traditional media (external) is necessary in improving ISA. Additionally, they argue that the use of external sources for informing employees even has a higher impact on ISA. With regards to the use of technology, Bawazir et al. (2016) recommend

to incorporate persuasive technology in the ISA program design and Mettouris, Maratou, Vuckovic, Papadopoulos, & Xenos (2015) propose to use 3D virtual worlds as a learning environment. In another research, Bauer et al. (2017) substantiate that many aspects of user's ISP compliance can be positively impacted through an extensive design of an ISA program, which should include media richness and customization of ISA interventions. In order to continuously increase the overall quality of the program, a PDCA cycle should be included with the process as well. Looking at the several aspects that should be taken into account, it's clear that there is a high level of complexity in creating an ISA program that helps in preventing ISP noncompliance (Bauer et al., 2017).

Bauer et al. (2017) have conducted qualitative research in several banking organization's regarding the design of ISA programs. A relevant finding for our research is that there are differences in ISP compliance between headquarters and branch employees, but unfortunately, it is not explicitly clear what these differences are. Despite this, they propose that organizations should take individual differences into account, by designing ISA programs tailored to specific types of users. Tailoring ISA programs to user groups is acknowledged by several other authors as well. Ki-Aries & Faily (2017) argue that the use of personas in ISA programs contributes positively to the level of employee's awareness. Tsohou, Karyda, & Kokolakis (2015) state that cultural biases should not be overlooked, and they recommended to create ISA programs for target groups based on applicable individual cultural biases. Furthermore, Chua, Wong, Low, & Chang (2018) claim that demographic characteristics of users should be taken in consideration, since the level of ISP compliance and awareness are dependent of three factors which include working industry, age and education level. In their research they state that a high level of ISP awareness was found within the financial industry and with people above the age of thirty, which supposedly have higher education than younger people. Remarkably, their claim regarding the relationship between age and educational level was not statistically proven. Diving deeper in the topic of age, several studies have found proof that this is an important factor in relation to ISA scores. Pattinson, Butavicius, Parsons, McCormac, & Calic (2015) suggested that older employees are more likely to have a lower risk-taking propensity, resulting in higher scores on ISA. In various other study's this suggestion has been confirmed (McCormac et al., 2017; Ögütçü, Testik, & Chouseinoglou, 2016; Wiley et al., 2020). In addition, Ögütçü et al. (2016) state that the level of ISA is strongly related to educational level and the study of McCormac et al. (2017) proved that females have a slightly higher ISA in comparison with males. However, evidence was found that the differences between males and females level out as age increases (Wiley et al., 2020).

Conclusion – Many studies have made it clear that individual differences are impacting ISA, and therefore it should be taken in consideration and incorporated in the creation of ISA programs. Doing this will improve employees in their knowledge and understanding of the organization's ISP, as well as their security mission.

2.2.3. How can users' ISA be measured? (1.c)

Measurement methods – As argued by several authors, increasing ISA amongst employees is successful with regards to increasing their ISP compliance (Bauer et al., 2017; Haeussinger & Kranz, 2013). However, a lack of metrics is frustrating organization's in performing ISA assessments (Bauer et al., 2017; Scholl, Leiner, & Fuhrmann, 2017). Honeypots (Christopher, Choo, & Dehghantanha, 2017) or the use of social engineering penetration tests (Bullée, Montoya, Pieters, Junger, & Hartel, 2015) can give insight in ISP compliant behavior. A downside is that invasive measures can have a negative impact on employee satisfaction (Bauer et al., 2017).

In order to measure the effect of ISA programs on the level of ISA, several methods can be used. Scholl et al. (2017) have given a generic overview of possible techniques, which include surveys, security incident monitoring and security experiments. When monitoring incidents, a disadvantage is that it won't give any insight in individual's level of ISA, but in general, it shows how the organization or department is performing as a whole. Scholl et al. (2017) also explain that security experiments, through e.g. sending fake phishing emails, are a means to observe staff behavior when they are actually confronted with a simulated attack on IS. It gives direct results on ISA of employees but can be costly and it can have negative effects on the organization's daily workflow. Additionally, and most importantly, it only gives insight in how an employee responds to phishing emails, and not in the individual's overall level of ISA. Lastly, the study showed that a survey is a common strategy for measuring employees ISA (Scholl et al., 2017). A survey strategy can involve a questionnaire, but also structured interviews and observations are belonging to this type of research (Saunders et al., 2016).

Several studies have measured ISA by using a survey approach, but these were focusing on only one area such as password management (Stanton, Stam, Mastrangelo, & Jolton, 2005). An instrument which covers a diversity of focus areas, is the Human Aspects of Information Security Questionnaire (HAIS-Q) (Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014).

Table 1: focus areas of Kruger & Kearney (2006)

Focus areas
Adhere to policies
Keep passwords secret
Email and internet
Mobile equipment
Report security incidents
Actions ⟹ consequences

HAIS-Q – Parsons et al. (2014) present the HAIS-Q, which gives insight in an employee's knowledge, attitude and behavior (KAB) regarding ISA in a working environment. The KAB model is a component of the HAIS-Q, which has formerly been discussed by Kruger & Kearney (2006) with regards to their prototype for ISA assessment. This prototype, based on several psychological models, measures ISA amongst the three KAB dimensions on several focus areas (table 1) by using a questionnaire. Parsons et al. (2014) developed the HAIS-Q in order to enable organizations to quantify ISA amongst employees. The HAIS-Q has also incorporated the KAB dimensions, which Parsons et al. (2014) define as follows:

- Knowledge: Knowledge of policy and procedures.
- Attitude: Attitude towards policy and procedures.
- Behavior: Self-reported behavior.

Despite the overlap with Kruger & Kearney's (2006) prototype on the KAB model, there is no importance weighting involved in the HAIS-Q. This choice has not been substantiated.

Parsons et al. (2014) explain further that in total seven focus areas (with each three sub-areas) have been formulated based on interviews with security managers and a review of organization's ISP's (table 2). The final questionnaire consists of 63 questions, since every sub-area consists of a knowledge, attitude and behavior statement. A five-point Likert scale is provided for answering the statements, ranging from Strongly Agree to Strongly Disagree. The HAIS-Q can be adapted to the requirements of the researcher since it is set up in a modular fashion, which means that not all seven focus areas or three dimensions have to be included, even though this would give the best insights in an individual's ISA (Parsons et al., 2017). In their paper, Parsons et al. (2014) explain that several factors such as demographics and organizational culture may influence KAB dimensions (fig. 2), which is also outlined by Tsohou et al. (2015) and confirmed through follow-up studies (McCormac et al., 2017; Wiley et al., 2020). Questions regarding these factors should be incorporated in the questionnaire in order to interpret the results of the individual's ISA scores, which can contribute to adapting ISA programs for specific groups, e.g. as part of a PDCA cycle (Bauer et al., 2017; Parsons et al., 2017). With a view to the sustainability of the HAIS-Q method, additional focus areas should be added based on the increase of threats and innovative technologies (Parsons et al., 2017).

Table 2: : focus areas and sub-areas of Parsons et al. (2014)

Focus areas	Sub-areas
Password management	Locking workstations Password sharing Choosing a good password
Email use	Forwarding emails Opening attachments IT department level of responsibility
Internet use	Installing unauthorized software Accessing dubious websites Inappropriate use of internet
Social networking site (SNS) use	Amount of work time spent on SNS Consequences of SNS Posting about work on SNS
Incident reporting	Reporting suspicious individuals Reporting bad behavior by colleagues Reporting all security incidents
Mobile computing	Physically securing personal electronic devices Sending sensitive information via mobile networks Checking work email via free network
Information handling	Disposing of sensitive documents Inserting DVDs/USB devices Leaving sensitive material unsecured

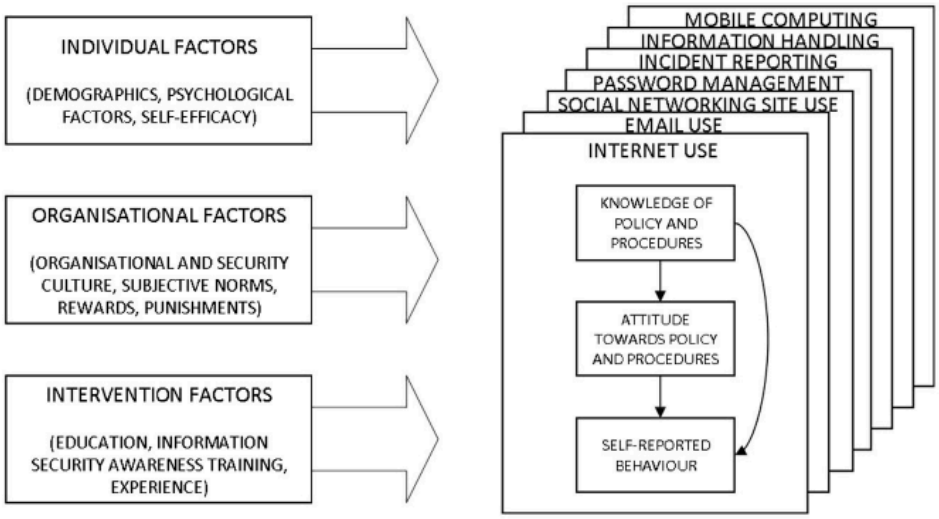

Figure 2: the HAIS model of Parsons et al. (2014)

The reliability and validity of the HAIS-Q has been validated through several studies (Hadlington & Chivers, 2018; McCormac et al., 2017; Parsons et al., 2017). In addition, it has been applied partly (only on the attitude and knowledge dimensions) among employees in the banking industry (Pattinson et al., 2016), but no distinction has been provided regarding the types of employees.

Conclusion – There are several methods to measure ISA. However, not all of them will provide a good insight on individuals ISA in a working environment. In order to cover a wide range of focus areas (which can be applied modularly), the HAIS-Q has been developed which measures those topics on knowledge, attitude and behavior dimensions. This validated questionnaire has been applied in several contexts, with amongst others, the banking industry.

2.3. Objective of the follow-up research

An extensive critical review has been carried out with a sufficient amount of literature, since a substantial amount of articles from key authors in the area of ISA have been analyzed (Saunders et al., 2016).
A clear conclusion that can be derived from the review, is that ISA programs should be tailored to specific types of users. To the best of our knowledge, only limited research has been carried out among employees in the banking industry. Since banks hold a lot of valuable information, this is a relevant context for conducting our follow-up research. Through a descriptive study on the awareness of two user groups, potential differences between them can be examined.

3. Methodology

3.1. Conceptual design

The literature review showed that limited research has been conducted regarding specific user groups in banking organizations. Providing insight in the differences between them contributes to the body of knowledge regarding ISA program design. Bauer et al.'s (2017) findings show that there are differences between branch and headquarter employees, but what these differences comprise is not clear. To clarify this, we have conducted a descriptive study. According to Saunders et al. (2016), this type of research can facilitate in retrieving profiles of two distinct groups of users, which in future studies might be e.g. statistically tested in an explanatory manner.

With a view to describing the differences, it was required to retrieve data from the two specific user groups regarding their level of ISA, in its real-life setting. Saunders et al. (2016) explain that for this type of research a cross-sectional, embedded single case study can be used. Single case, since it's conducted in one organization, and embedded, because two different units of analysis are used (i.e. each user group is one unit of analysis). A case refers in this case to a banking organization in The Netherlands. The timeframe is for this project was tight, and therefore we chose to conduct a cross-sectional case study. Within a case study, a mixed methods design was applied since it benefits the research, by e.g. combining interviews, observations, focus groups and/or questionnaires. Through our inductive approach, the results of this case study formed a basis for further research (Saunders et al., 2016).

For our research project we applied a mixed method design by using both the (semi-structured) focus group interview and questionnaire as part of our case study strategy. Despite the fact that it is very frequently used, Saunders et al. (2016) explain that questionnaires fit well with our aim to identify differences within organizational practices. Our choice to what type of questionnaire to be used (postal questionnaire, mobile questionnaire, structured interviews etc.) depended on a.o. the number of questions, type of questions and size of the sample. With regards to the questionnaire, the sample is a part of the population, and the respondents are the people that actually participated in the questionnaire (Doorewaard & Tjemkes, 2019). An important reason for applying a mixed methods design, is that we wanted to come to a good set of questionnaire items, as well as to get an understanding of the contextual background. In addition, we wanted to ask our questions in a natural manner, without sticking to a very tight structure. A semi-structured interview offered this opportunity (Saunders et al., 2016). A disadvantage is that an interview may be time consuming (Saunders et al., 2016), but in our opinion, this weights up to the advantages. As a result of the semi-structured group interview, the HAIS-Q as we wanted to apply it could be finalized.

3.2. Technical design

3.2.1. Case study organization

As described in paragraph 3.1, a cross-sectional, embedded single case study was carried out for this project. A first step was to determine the case study organization and the sub-units that would be examined. The empirical part of this study was performed in two sub-units within a banking organization in the Netherlands. Here, we have selected units that are differing from one another to a major extent with regards to roles, daily operations and responsibilities. This enabled us to write clear conclusions on results, and to provide propositions that can be tested in future research.

The case study organization is one of the largest banks in the Netherlands, hereafter referred to as Bank X. Bank X is active in both private and business banking, with a full range of products (payments, savings, insurance, lending etc.). The two selected sub-units are headquarters and branch employees. The sub-units are defined as follows:

Sub-unit 1: Headquarters employees (in this research also referred to as head office employees) are working on locations that are mostly not open for clients and they explicitly don't have any direct client contact or client responsibility. These people are primarily policy makers, marketing employees, HR employees, IT-related personnel or higher management. The majority of the employees work on one central location in the Netherlands.

Sub-unit 2: Branch employees (in this research also referred to as local bank employees) have daily client contact through multiple channels, such as e-mail, phone, chat and face-to-face. The working locations involve centralized client contact centers and local walk-in offices for daily banking purposes, business or private banking. The employees have direct client contact on a daily basis and are working throughout the Netherlands on many different locations (based on their area of residence).

3.2.2. Determining the HAIS-Q

The HAIS-Q can be found in appendix 2, but as outlined in paragraph 2.2.3, the HAIS-Q can be applied modularly. Parsons et al. (2014) indicated that filling out the questionnaire in their pilot and main study took respectively 18 and 37 minutes on average. To minimize non-response because of e.g. discouragement, we were aiming to shorten the HAIS-Q. According to Doorewaard & Tjemkes (2019), one should try to work to a completion time of 10 minutes. However, we also wanted to collect as much relevant data as possible, thus we sought for a good balance between completion time and data to be collected. To guide us in making choices regarding which topics/dimensions to include, we have conducted a focus group interview with two Information Security Specialists of Bank X. Both people have extensive experience in the field of IS, and were therefore expected to be able to give relevant input. Saunders et al. (2016) explain that group interviews, where both members are encouraged by the interviewer to answer freely to the questions, can result in a high-quality discussion with a fruitful outcome. Another benefit is that the discussion would not be limited like in one-to-one interviews, and also, it could help in the identification of focus areas which should be part of the HAIS-Q. During the focus group interview the main emphasis was on a specific topic, i.e. the determination of the HAIS-Q. Our task was to act as a facilitator which should keep the discussion within the limits of the topic and to encourage attendees to openly discuss their views (Saunders et al., 2016).

3.2.3. Data collection through the HAIS-Q

After the focus group interview, the selection of the focus areas/dimensions took place and the questionnaire could be finalized. Several types of questionnaires can be applied, e.g. postal or telephone questionnaires (Saunders et al., 2016), but we followed previous studies (e.g. Hadlington & Chivers, 2018; Parsons et al., 2017, 2014; Pattinson et al., 2016) where the HAIS-Q was applied through the online channel (web questionnaire). Saunders et al. (2016) describe that the web questionnaires can handle a large sample size, and that it is suitable for people who have access to e-mail. Doorewaard & Tjemkes (2019) add that in this way, data collection can be carried out in a relatively short period of time, and by using questionnaire software its look and feel can be designed to increase response. Since LimeSurvey (https://www.limesurvey.org) offers this opportunity, we chose their services for exposing our questionnaire.

In order to further increase the response rate, reliability and validity, it is recommended to take extra steps. Saunders et al. (2016) explain that, in addition to the visual design, attention should be paid to the explanation of the purpose of the research, pilot testing and a carefully planned script for sending and receiving questionnaires. Since the HAIS-Q is an existing questionnaire of which its validity and reliability has been proven multiple times in former studies, no adaptions have been made (other than those related to the modular fashion of the instrument). For the same reason, we found it acceptable to proceed without pilot testing. However, we provided a clear explanation of the purpose of the questionnaire and ensured that it is visually attractive to the respondents. The questionnaire was accessible for three weeks after sending the invitation. One reminder has been sent during this period of time after approximately one week, as recommended by Saunders et al. (2016).

3.3. Data analysis

This study consists of a focus group interview and a questionnaire. However, the interview did not have the goal to explore or explain a certain topic or phenomenon since it was primarily held in order to select topics/dimensions that should be included in the HAIS-Q. In other words, the focus group interview wasn't intended to provide answer to the research questions. Nevertheless, we aimed to follow a structured approach for analyzing the data that evolved from the interview, and therefore we applied a Thematic Analysis. Saunders et al. (2016) explain that the Thematic Analysis allows to code the data and to draw and verify conclusions on the key themes.

The analysis of the quantitative data that evolves from the questionnaire is analyzed using a statistics computer programme (SPSS). The HAIS-Q consists of questions based on a five-point Likert scale, and Saunders et al. (2016) explain that this categorical data is to be considered ranked (ordinal) data, where non-parametric statistics need to be applied. We are mainly interested in the differences between the two specific groups, and we therefore performed tests to determine if these differences exist. Looking at the type of data and the scope of this research, The Mann-Whitney U Test enabled us to execute the comparison of those groups (Nachar, 2008).

3.4. Validity, reliability and ethical aspects

3.4.1. Validity and reliability of the HAIS-Q

When speaking about reliability, it's all about to what extent the research is consistent and can be replicated (Saunders et al., 2016). To reach an acceptable level of reliability, this research aims to give insight in the choices that are being made, with a clear substantiation of these choices. All the data that evolved from the interview and questionnaire has been stored in a database. This includes raw data (recordings), a transcription of the interview, a raw data set of the questionnaire results and all other

data and information that helped in forming this paper. LimeSurvey was used from the Open University server for reproducibility purposes, which contributed to reliability of this study. While conducting the interview, we were aware of risks to reliability such as researcher bias (Saunders et al., 2016), since we did not want to influence the responses of the interviewees. To ensure that the data from the questionnaire was consistent, the Cronbach's alpha was used for determining internal reliability (Saunders et al., 2016). However, before doing this, the data needed to be normalized because on a number of questions reverse scoring is applied (Parsons et al., 2017).

The level of ISA was to be measured through an existing questionnaire that already has been validated multiple times in former studies. According to Parsons et al. (2014), several steps were taken during the initial development of the HAIS-Q for ensuring a high level of validity. The questionnaire has been created with the input of an expert which pre-tested the tool, before it was presented to a pilot group. The pilot group was carefully selected and respondents that e.g. did not have an ISP at their organization were excluded. This approach is in line with Saunders et al. (2016) and Doorewaard & Tjemkes (2019) who argue that involving other individuals contributes to content and face validity. Saunders et al. (2016) also explain that when relationships between variables are to be measured, in this case for attitude, knowledge, behavior, the Pearson's product moment correlation tests can be applied. The results of this test, as well as the outcomes of the expert session, the pilot group session and the main study have been processed in the HAIS-Q which has been used in follow-up studies. For example by Parsons et al. (2017), who have shown proof for the convergent validity by comparing results of a phishing experiment and the HAIS-Q on several user groups. In the analysis of their findings, Parsons et al. (2017) found limited proof for socially desirable answering. Although this has been substantiated as plausible by the authors, this is an important indicator that should not be overlooked.

With regards to reliability, Cronbach's alpha showed good internal consistency (e.g. McCormac et al., 2016, 2017; Parsons et al., 2017, 2014; Pattinson et al., 2016; Wiley et al., 2020). Since we aimed to apply a shortened version of the HAIS-Q, it is good to know that in this case also a high level of consistency was proven (Hadlington & Chivers, 2018).

3.4.2. Ethical aspects

Ethical aspects are of paramount importance to us. Therefore, we conducted our research with the ethical principles, as described by Saunders et al. (2016), in mind: being integer and objectively, while respecting others and avoiding harm to the participants. As members of the Open University, we in addition followed the ethical principles as provided in the Master Thesis Handbook (Counotte-Potman, Kusters, & Joosten, 2019). Both the interview and questionnaire were presented to interviewees/respondents with a clear explanation of how their responses will be processed. It has been explained that taking part is always voluntarily and all participants retain the right to withdraw from our study when this is requested. We agree with Saunders et al. (2016) that the information we obtained is key, not the individual that provided it. Therefore, we aimed to maintain anonymity of the case study company, interviewees and respondents by using pseudonyms in this paper and handling their information in a confidential matter.

4. Results

4.1. Determining the R-HAIS-Q

In the initial stage of the empirical research a semi-structured focus group interview took place in order to determine a reduced set of questions of the HAIS-Q, which we refer to as the R-HAIS-Q. For determining the R-HAIS-Q, we followed Saunders et al. (2016) on their approach regarding preparation and conducting the interview.

4.1.1. Preparation

The empirical part of this research has been started after a period of intensive study on academic material regarding ISA. Therefore, the level of knowledge of the interviewer regarding ISA was sufficient for conducting the interview. The company's annual report has been read in order to have a good general understanding of the organization. Since all attendants of the interview were Dutch, cultural differences were considered to be minimal.

Since the main goal of the focus group interview was to determine the R-HAIS-Q, we provided the interviewees with the HAIS-Q (appendix 2, including focus areas, sub-areas, KAB dimensions and statements) several days before the interview. To ensure a safe and convenient environment during the interview, it took place within the researched organization in a quiet, comfortable meeting room where it was unlikely to be interrupted. In addition, a note was posted on the door of the room requesting unexpected visitors not to disturb.

Saunders et al. (2016) recommend providing an information sheet with several aspects regarding the research (e.g. nature, rights of those taking part, use of collected data) to reach informed consent. We have followed this recommendation. The information sheet can be found in appendix 3.

Opening the interview – Before starting the main part of the interview, we provided the interviewees with a brief explanation of the research. In addition, we specifically requested for consent and open questions were answered. An explanation of the HAIS-Q was given, with a special focus on how it can be applied modularly. The following topics were involved in the opening of the interview:

- Welcome;
- Purpose and brief explanation of the research;
- General explanation of the HAIS-Q, including the possibility for modular application;
- Consent;
- Informal discussion (e.g. about roles of the interviewees at the organization).

Conducting the interview: the main section – After opening the interview, we initiated the main section. First, we are aimed to get insight in the contextual background, i.e. the current situation and efforts regarding ISA. Subsequently, we followed a step-by-step approach through the list of focus areas where the interviewees were asked if it should be part of the questionnaire (or not). This section included the following questions:

- How would you describe the current situation of your organization regarding ISA?
- To what extent is the organization taking steps to increase ISA?
    - Probing question: how is the organization doing this?
- For every focus area, the following questions are presented:
    - Should '*focus area'* (e.g. password management) be part of the questionnaire?
        a. Probing question: why yes? Or why not?

Closing the interview – The interview was summarized by concluding if and how, to the interviewee's professional opinion, the HAIS-Q could be reduced. Accordingly, the respondents were thanked for their participation and the information they have shared with us.

4.1.2. Approach for analysis of the interview

As explained earlier in this paper, the main goal was to get familiar with the contextual background and to come to a final selection of focus areas that should be part of the R-HAIS-Q. The Thematic Analysis is primarily used to thoroughly analyze the qualitative data in order to ultimately recognize relations and to test propositions (Saunders et al., 2016). This is not in line of the purpose of our interview, however, several steps provided by the authors were useful for our analysis. Those steps involve the transcription of the interview and coding of the qualitative data. During the interview, a record has been made with two devices in order to ensure a (good quality) record. Additionally, as advised by Saunders et al. (2016), notes were made during the interview in order to maintain focused and to make sure that all discussion points were covered.

Transcription – Transcribing the recorded interview is a way to prepare the qualitative data for analysis, and to become familiar with the data (Saunders et al., 2016). As indicated by the authors, transcribing the interview can be time consuming, therefore we applied one of the recommended alternative ways to reduce transcription time. Online research showed that Trint (http://www.trint.com) offers online voice-recognition software which supports the format of the file (.m4a). After the automatic transcription was carried out, the full interview has been carefully checked on accuracy and corrected where needed. The full transcript is available upon request.

Coding – Coding can applied in order to easily recognize the pieces of data that are relevant for our analysis (Saunders et al., 2016). Therefore, we applied this method on our transcribed interview. The main purpose was to label the parts of the interview where the focus areas were discussed. Every focus area was used as a label to the relevant units of data in the transcript. E.g., the unit of analysis where focus area 'password management' was discussed, has been labelled as 'password management'. This enabled us to efficiently extract conclusions from the total set of qualitative data (Saunders et al., 2016).

4.1.3. Interview results

The interview has been conducted with two ISA specialists that are employed with Bank X. Their introduction has shown that both have long experience with regards to awareness. At the moment of the interview, Specialist A (Policy Standards Advisor) has been working several years with Bank X, and his primary task was to create strategic solutions and a network to increase awareness of employees. Specialist B has recently started as Digital Security Advisor and has, prior to her current role, been focusing on customer awareness (i.e. awareness of users of internet banking, mobile banking) within Bank X. Both employees have the responsibility to reach a higher level of awareness among users within the organization. Specialist B mentioned that this does not only apply for information security awareness, but also for e.g. privacy awareness and business continuity awareness.

A benefit of this focus group interview was that both interviewees complemented each other in several discussions. Specialist A has more working experience in this area of awareness than Specialist B, which in some cases provided an interesting discussion between them. However, our observation was also that Specialist A had a more dominant role in the discussions, presumably because of his experience. We aimed to let both interviewees finish their points made, in order to have a meaningful contribution to purpose of this interview.

Contextual background – As part of the interview, insight has been gained on the current ISA efforts that Bank X undertakes. Two years ago, the organization started off with a program that is meant to eliminate security threats to the organization. This project was directly supported by the managing board, which emphasizes the importance of the program to Bank X. The forming of the strategy and approach resulted in a program that consists of two pillars; baseline security awareness and target groups awareness. Baseline security awareness is applicable to all people working for Bank X, which consists of four categories (a.o. social engineering, secure communication) and target group awareness is applicable for eight specified groups of employees (a.o. CEO's, management staff, developers, service desks). Specialist A explained that information for these groups is specific and mostly not applicable for ordinary employees, hence the choice has been made to provide this information only to the specific target groups.

An important change that Bank X wanted to make was to let people experience security as something positive. They emphasized that this is part of working on the network, creating people that act as stakeholders. E-learnings are used as a very basic tool for increasing awareness, but according to Specialist B *"change of behavior will never be reached by an e-learning"*. Bank X tries to generate a change in behavior by providing a personal experience (through a combination of methods, such as e-learning and an event). Channels are used with the right mix and balance, such as regular corporate channels (e-mail, newsletters), but if necessary, also other channels are used. In an example, Specialist A explains that the target group 'developers' were not able to be reached through standard channels, and they are therefore using Slack as an alternative (with hyperlinks to approved tooling in a secure environment). In the end, communicating ISA information through several channels should help in effectively reaching the employees. The interviewees underlined a lack of metrics that can be used for assessing ISA and are currently only using a phishing test. Looking at the future, they mentioned that ISA is more top of mind now, and that users are proactively contacting security officers for ISA related questions and concerns.

Selection of focus areas – An interesting discussion was initiated by going through all the focus areas that are present in the original HAIS-Q. The focus areas that according to the interviewees could be excluded, are ranked as follows:

1. Focus area: internet use
   Main reason for the interviewees to remove this focus area can be found in the preventive technical measures that the organization is already taking. Higher risk websites with explicit content are blocked, and files cannot be installed without approval of a system administrator. This means that most statements are not applicable within the research environment.
2. Focus area: information handling
   The interviewees argued that this focus area is less relevant, because sensitive material and sensitive printouts are hardly used anymore, especially for headquarters employees. Local banks may hold some sensitive documents (e.g. contracts, agreements), but most of them are distributed and signed through internet banking these days. With regards to removable media, both interviewees were not able to argue the relevance of this topic. Therefore, interviewees referred us to another department. A representative (Security Officer) explained that USB-sticks are read-only, the system blocks potential malicious software, and live monitoring is applicable through logging of end-point protection. Nevertheless, they argue that these measures are not watertight.

3. Focus area: social media use
   The only reason why, according to the interviewees, this focus area should be removed, is because some social media channels are used within the (secure) working environment. Yammer (http://www.yammer.com) is used for internal communication (Bank X approved channel), and GitHub (http://www.github.com) and Slack (http://www.slack.com) are used by developers. They recommend adding an explanation to the focus area, where it is made clear that statements apply to personal social network accounts.

Looking at the argumentation and recommendations of the interviewees, we have chosen to exclude the focus areas 'internet use' and 'information handling' from the HAIS-Q for our empirical research. For the focus area 'social media use' it took only little effort to give clarification of the topic to the respondents. For 'internet use' and 'information handling', many statements can be regarded as not applicable within the organization. The focus areas that are included in the R-HAIS-Q are presented in table 3.

Table 3: R-HAIS-Q

Focus areas	Sub-areas
Password management	Using the same password Sharing passwords Using a strong password
Email use	Clicking on links in emails from known senders Clicking on links in emails from unknown senders Opening attachments in emails from unknown senders
Social media use	SM privacy settings Considering consequences Posting about work
Mobile devices	Physically securing mobile devices Sending sensitive information via WIFI Shoulder surfing
Incident reporting	Reporting suspicious behaviour Ignoring poor security behaviour by colleagues Reporting all incidents

4.2. R-HAIS-Q

4.2.1. Creation and application

The R-HAIS-Q has been created using the LimeSurvey (http://www.limesurvey.org) platform. We have followed the recommendations of Parsons et al. (2017) in the set-up of the questionnaire. First, we have introduced the instrument to the respondents by explaining what the questions are about. Subsequently, we have presented the statements in three different sets of questions (knowledge, attitude, behavior). The sets of questions have been introduced by describing what is meant with the respective dimension. Within the sets of questions, we placed the statements in a fixed-random order and 23 statements have been negatively worded (reverse scoring). In addition to the 45 statements, we have incorporated questions regarding gender, age, educational level and working environment. To every statement, it was possible to select the 'no answer' or 'not applicable' option. An overview of the setup and settings of the R-HAIS-Q can be found in appendix 5, and the full questionnaire can be found in appendix 6.

4.2.2. Self-selection sampling

It would have been impossible to retrieve a completely filled in R-HAIS-Q by all employees within the headquarter and branch population. In order to work with a sub-group, we've applied a sampling technique (Saunders et al., 2016). Because not all headquarter and branch employees in the Netherlands were deemed to be easily accessible, we defined a target population of which we have drawn samples. The target populations are outlined in paragraph 3.2.1.

We looked into what actually is practically possible in our study. Due to the lack of a complete list with employees belonging to both target populations (i.e. a sampling frame), we decided to apply a non-probability sampling technique. This is supported by Saunders et al. (2016), who justify that self-selection sampling is a technique that matches these circumstances. It primarily fits well since access

to both groups was expected to be fairly challenging. Downside to this approach is that the likelihood of representativeness is rather low, which influences statistical inferences made.

The invitation for filling in the questionnaire has been sent to 56 headquarters and 300 branch employees, by email. Since branch employees are spread through the country, we decided to approach a more extensive group of branch employees than headquarter employees. We did this by selecting branches located in both urban and provincial/sub-urban areas, which contributes to a consistent group of branch employees. The selected headquarter employees are working on one central location in the Netherlands, primarily in (product) management, IT and process management. Regarding branch employees, we have selected those who are working in private and business banking departments, where the chances of working with clients on a daily basis were expected to be high.

As explained by Saunders et al. (2016), for most non-probability sampling techniques there aren't specific guidelines or rules with regards to the sample size. Looking at the nature of our descriptive research, the selected sample sizes were able to give substance to our research questions.

4.2.3. Plan for analysis of results

The plan for the analysis of the results can be found in appendix 4, which has been applied as we intended.

4.3. R-HAIS-Q: collected data

The questionnaire was active from April 7th, 2020 until April 22nd, 2020. In total, 71 respondents have completed the questionnaire, and 16 questionnaires have been filled partially.

4.3.1. Partially filled questionnaires

Partially filled questionnaires have not been included in the analysis, since this influences the consistency of the results. Below we provide an analysis on which we based this decision:

- Regarding working location: the majority of partially filled questionnaires came from branch users (nine), and two respondents selected the 'no answer' option. Another two respondents did not complete this question, and three partially filled questionnaires came from headquarter employees.
- Ten out of sixteen questionnaires have been closed after the general questions, without answering to any of the KAB statements;
- Six respondents answered only to the first fifteen (knowledge) statements;
- Four of these respondents continued to the next set of fifteen (attitude) statements. However, one of these respondents answered 'No answer' to all attitude statements;
- None of the sixteen partially filled questionnaires contained answers to the behavior statements.

4.3.2. Response rate

As outlined in paragraph 4.2.2, we expressed that we've sent the questionnaire to a more extensive group of branch employees than headquarter employees. The response rates per sub-unit and the total response rate are presented in table 4. One respondent could not be classified to either headquarter or branch employee groups (paragraph 4.3.3). Hence, this respondent is not included in the response rate table.

Table 4: response rates

Response rate	Headquarter employees		Branch employees		All employees	
	Total number of responses	Total number in sample	Total number of responses	Total number in sample	Total number of responses	Total number in sample
	36	56	34	300	70	356
Response rate:	**64,29%**		**11,33%**		**19,66%**	

4.3.3. Quality of collected data

As mentioned in paragraph 4.2.3, we first assessed the quality of the collected data. Here, we are presenting our findings, (if applicable) actions taken and an argumentation.

- Regarding non-responsivity, there were no respondents that provided the same answer to every question;
- One respondent selected the 'No answer' option to both the questions 'Where do you work?' and 'To what extent do you have contact with clients?'. This response has been excluded from the results, which has two reasons. First, the answers suggested that the respondent possibly didn't work at the organization. Secondly, these answers made this response meaningless to this research, since we aimed to find differences between headquarters and branch employees;
- As explained in paragraph 3.2.1, our intention with this research is to explore if differences can be found on ISA between headquarter and branch employees. We elaborated on these sub-units by specifying to what extent they have client contact. To ensure that we were only analyzing both these user groups, we asked our respondents to what extent they have contact with clients contact (figure 3).

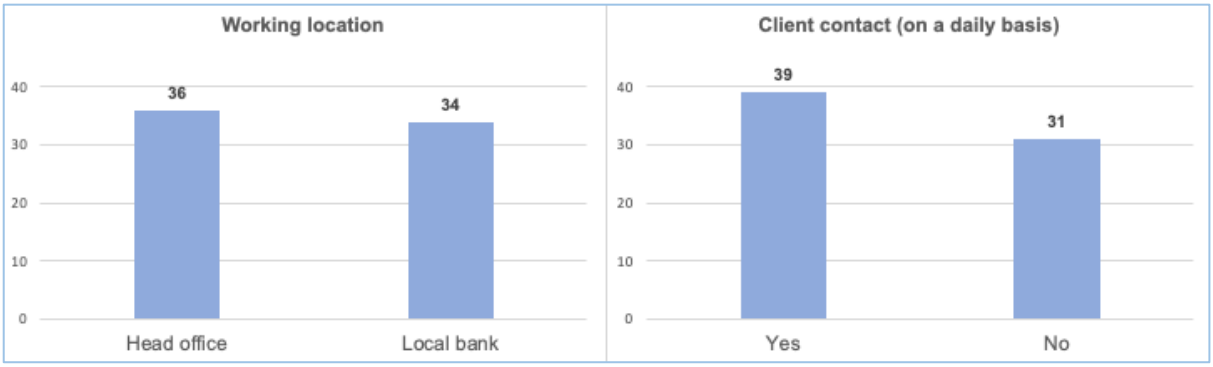

Figure 3: Respondents working location and client contact

Our analysis of the respondents showed that all branch employees do have client contact on a daily basis. However, five respondents that answered 'head office' to the working location question, also indicated that they have client contact on a daily basis. Since those respondents do not fit in the headquarter employee user group (as we describe in our research), they were not included in the further analyses.

The questionnaire results of the 65 remaining respondents (which are used for further analysis), can be found in appendix 7.

4.4. R-HAIS-Q results

First, we describe the general (demographic) information of the respondents as well as the internal reliability of the R-HAIS-Q. Subsequently, we present the ISA scores of both user groups (4.4.4), which is followed by a detailed analysis of the differences on ISA.

4.4.1. Respondents' demographics

In figure 4, we have visualized the demographic details of the respondents. The majority of the respondents are male, aged between 26 and 40, and are mainly equipped with higher professional education. There were no respondents aged 69 years or older.

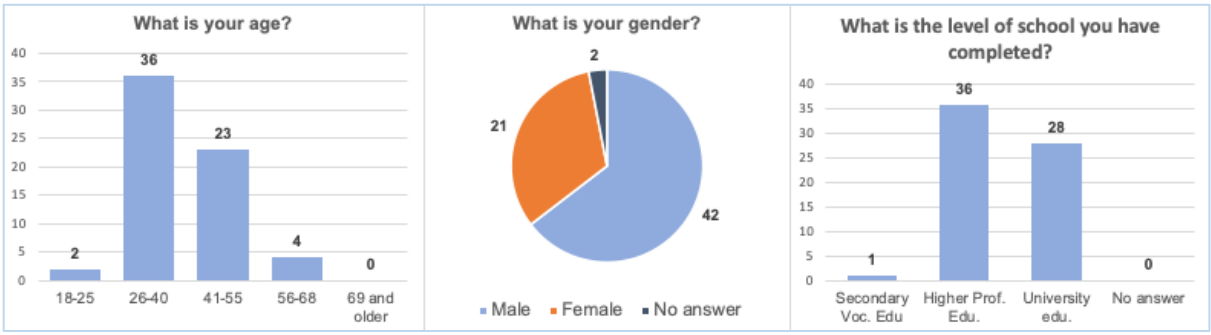

Figure 4: Respondents age, gender & educational level

4.4.2. Reliability of the R-HAIS-Q

We calculated Cronbach's alpha for overall ISA, each KAB dimension and each focus area in order to assess internal reliability (table 5 & 6). The results show that the attitude and behavior dimensions are exceeding the recommended Cronbach's alpha value of 0.7 (Saunders et al., 2016). This indicates that within these dimensions we are measuring what we intend to measure. However, knowledge is far below this value and unfortunately, our analysis on this didn't lead to a clear-cut explanation. I.e., there are no specific items in the knowledge dimension that lead to this low internal reliability score. With regards to overall ISA, Cronbach's alpha is exceeding the recommended Cronbach's alpha value.

Table 5: internal reliability on KAB dimensions & overall ISA

Cronbach's alpha (KAB dimensions & overall ISA)	
Knowledge of policy and procedures	.494
Attitude towards policy and procedures	.740
Self-reported behavior	.791
Overall ISA	.857

Next, we calculated Cronbach's alpha for each focus area. Here we can see that password management and incident reporting are exceeding the recommended Cronbach's alpha value of 0.7 (Saunders et al., 2016), but this does not count for the other three focus areas. In order to increase the internal reliability of those focus areas, several items have been deleted. However, in all three cases the alpha value of 0.7 could not be exceeded. The items that are deleted, are the following (including code and KAB dimension:

- Email use
  - 'I am allowed to click on any links in emails from people I know' (KNE04, knowledge)
  - 'I am not permitted to click on a link in an email from an unknown sender' (KNE05, knowledge).
  - 'I am allowed to open email attachments from unknown senders' (KNE06, knowledge).
  - 'I don't always click on links in emails just because they come from someone I know (BEE04, behavior).

- Social media use
    - ‘It doesn't matter if I post things on social media that I wouldn't normally say in public’ (ATS08, attitude).
    - ‘I can post what I want about work on social media’ (KNS09, knowledge).
- Mobile devices
    - ‘When working in a public place, I have to keep my laptop with me at all times’ (KNM10, knowledge).

Here also, we can see that deleted items are primarily knowledge items. Therefore, we took the following decisions proceeding forward. With regards to our matrix in paragraph 4.4.4, we decided to calculate ISA based on only the attitude and behavior dimension. In addition, we excluded the statements that contributed to lower internal reliability. Since email use, social media use and mobile devices are nearly meeting the recommended Cronbach’s alpha value, we decided to include these focus areas in the matrix for an indication of ISA scores. However, it does not allow us to draw reliable conclusions on these particular concept levels.

Table 6: internal reliability on focus areas

Cronbach's alpha (focus areas)	
Password management	.717
Email use	.550
Social media use	.607
Mobile devices	.637
Incident reporting	.759

Cronbach's alpha (focus areas, with items deleted)	
Password management	.717
Email use	.690
Social media use	.683
Mobile devices	.698
Incident reporting	.759

4.4.3. ISA score calculation

Pattinson et al. (2016) have explained their method to calculate an ISA score, where ‘strongly agree’ and ‘agree’ answers are expressed in a positive ISA value. Since (most of) these authors are also the creators of the HAIS-Q we decided to follow their formula:

$$ISA\ \% = \frac{Strongly\ agree\ answers + Agree\ answers}{Number\ of\ responses - Not\ applicable\ answers}$$

To calculate a total score on e.g. the password management focus area, we used the average over attitude and behavior scores. We will go through every focus area by analyzing the statements belonging to that particular area in paragraph 4.4.5.

4.4.4. Employee group differences

After taking steps with regards to internal reliability (paragraph 4.4.2), a matrix is created regarding the scores of both user groups on a general level (table 7). In addition to the matrix, we also present a visualization of the scores in figure 5.

In general, we can see that headquarter employees are scoring higher on password management, email use and social media use focus areas. This results in a higher overall score for this group compared to branch users, who are showing higher scores on incident reporting and mobile devices. If we take a closer look at both user groups, we can see that relatively large differences can be observed within the password management and social media use focus areas.

Table 7: matrix on headquarter and branch employee ISA

	Headquarter employees			Branch employees		
	Attitude	Behavior	ISA	Attitude	Behavior	ISA
Password management	97	93	95	88	87	88
Email use	96	94	95	97	85	91
Social media use	97	87	92	87	78	82
Mobile devices	96	93	95	97	94	96
Incident reporting	97	86	91	94	89	92
Overall	96	91	94	93	87	90

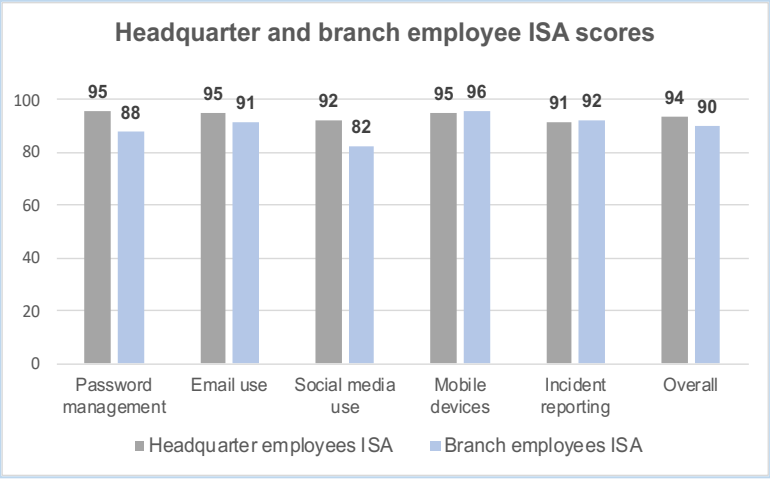

Figure 5: graph on headquarter and branch employees ISA scores

4.4.5. Employee group differences on focus area level

In this section, we dive deeper in the results of the questionnaire and we do this by handling the statements (where we have found significant differences) separately. In the previous paragraph, we excluded several statements and the complete knowledge dimension since Cronbach's alpha didn't demonstrate internal reliability for that particular concept (i.e. dimension or focus area). However, since we are investigating on statement levels what the observed differences are, we included all statements in this part of the analysis.

In accordance with paragraph 4.4.3, we extended our approach in performing the Mann Whitney U tests. This means that we marked "strongly agree" and "agree" responses as favorable with regards to ISA scores. This is in line with Pattinson et al. (2016), who are the authors of both the HAIS-Q and the method for calculating an ISA score. For every focus area, we performed the Mann Whitney U test on the individual statements.

For analyzing differences we used the Mann Whitney U test considering that we want to compare two independent samples of ordinal data (Allen, Bennett, & King, 2010). The overview of test results is showing a number of statistics, which include:

- **Mann-Whitney U –** This statistic indicates the differences between the two groups, where a value of 0 means that they are completely differing from one another (Allen et al., 2010).
- **Wilcoxon W –** The Wilcoxon rank sum (*W)* statistic; an equivalent to the Mann Whitney U test. The value shown is the rank sum of the smaller group (Field, 2013);

- **Z –** In our research, the normally distributed *Z* statistic is transformed from *U*, where *Z* is corrected for ties (http://www.ibm.com). The *Z* statistic is used to assess statistical significance (Allen et al., 2010).
- **Asymp. Sig (2-tailed) –** I.e. the two-tailed asymptotic probability of *Z* (Allen et al., 2010). If this *p*-value, i.e. asymptotic significance (2-tailed), is lower than .05, it can be concluded that there is a statistical significant difference between the headquarter and branch employees (Field, 2013).

We have found significant differences between the two employee groups within the focus areas password management, email use and social media use. The results of these focus areas are presented in table 8, where we have highlighted the statements where significant differences have been found. A complete presentation of the test results of all five focus areas can be found in appendix 8. First, we present the findings within the password management focus area:

Password management – The following statement, belonging to the 'Using a strong password' sub-area, showed a significant difference between the two groups:

- 8. 'It's safe to have a work password with just letters' (attitude)
  The test on this statement indicated that the awareness levels of headquarter employees (*Mean Rank* = 36.45*, n* = 31*)* were significantly higher than those of branch employees (*Mean Rank* = 29.85, *n* = 34), *U* = 420.00, *z* = -2.35 (corrected for ties), *p* = .019, two-tailed.

Despite the fact that we found a significant difference (in favor of headquarter employees) on attitude, this isn't reflected within the related knowledge and self-reported behavior statements belonging to this sub-area (respectively statement 7 and 9 in table 8).

Email use – Three statements are showing significant differences between both groups. Two statements belong to the 'Clicking on links in emails from unknown senders' subarea:

- 4. 'I am not permitted to click on a link in an email from an unknown sender' (knowledge)
  The test on this statement indicated that the awareness levels of branch employees (*Mean Rank* = 36.18, *n* = 34) differ significantly from those of headquarter employees (*Mean Rank* = 29.52, *n* = 31), *U* = 419.00, *z* = -1.99 (corrected for ties), *p* = 0.46, two-tailed.
- 6. 'If an email from an unknown sender looks interesting, I click on a link within it' (behavior)
  Interestingly, here we can see that the awareness levels of headquarter employees (*Mean Rank* = 35.50, *n* = 31) are higher than those of branch employees (*Mean Rank* = 30.72, *n* = 34), *U* = 449.50, *z* = -2.21 (corrected for ties), *p* = .027, two-tailed.

These results provide an interesting insight. Branch employees have significantly higher knowledge regarding clicking on links in emails from unknown senders, while their counterparts are showing significantly better self-reported behavior in this matter. Looking at the attitude statement within this sub-area (5. 'Nothing bad can happen if I click on a link in an email from an unknown sender'), both user groups are showing no differences, while scoring 100%.

The following statement is part of the 'Opening attachments in emails from unknown senders' sub-area:

- 7. 'I am allowed to open email attachments from unknown senders' (knowledge)
  Here, the test results also show that the awareness levels of branch employees (*Mean Rank* = 35.50, *n* = 34) differ significantly from those of headquarter employees (*Mean Rank* = 30.26, *n* = 31), *U* = 442.00, *z* = - 2.42 (corrected for ties), *p* = .016, two-tailed.

Here also, branch users are showing better knowledge regarding emails from unknown senders. Despite this, no significant differences are found on the related behavior statement (9. 'I don't open email attachments if the sender is unknown to me').

Social media use – Three statements show significant differences. Two statements belong to the 'Social media privacy settings' sub-area:

- 2. 'It's a good idea to regularly review my social media privacy settings' (attitude)
  In this case, headquarter employees (*Mean Rank* = 34.89, *n* = 28) differ significantly from branch employees (*Mean Rank* = 28.71, *n* = 34), *U* = 381.00, *z* = -2.20 (corrected for ties), *p* = .028, two-tailed.
- 3. 'I don't regularly review my social media privacy settings (behavior)
  Here also, a significant difference can be found in favor of headquarter employees (*Mean Rank* = 35.70, *n* = 28) versus branch employees (*Mean Rank* = 27.02, *n* = 33), *U* = 330.50, *z* = -2.20 (corrected for ties), *p* = 0.28, two-tailed.

Despite the fact that no significant differences are found regarding the knowledge-part of this sub-area, the attitude and behavior statements show that headquarter employees are more aware regarding this topic than branch employees.

The following statement where significant differences were observed belongs to the 'Considering consequences' sub-area:

- 4. 'I can't be fired for something I post on social media' (knowledge)
  With regards to this statement, there is a significant difference between headquarter employees (*Mean Rank* = 39.85, *n* = 31) and branch employees (*Mean Rank* = 26.75, *n* = 34), *U* = 314.50, *z* = -3.49 (corrected for ties), *p* = .000, two-tailed.

Similar to the 'Social media privacy settings' sub-area, in this case also the headquarter employees are showing significant higher awareness levels. However, at the same time there are no significant differences observable regarding the related attitude and behavior statements.

Table 8: Mann Whitney U test results - Password management, Email use and Social media use

Mann Whitney U test - Password Management

					Headquarter employees			Branch employees			Test statistics			
Nr.	Code:	KAB dimension	Sub-area	Statement	N	Mean Rank	Sum of Ranks	N	Mean Rank	Sum of Ranks	Mann Whitney U	Wilcoxon W	Z	Asymp. Sig. (2-tailed)
1	KNP01	Knowledge	Using the same password	It's acceptable to use my social media passwords on my work accounts.	31	34.97	1084.00	33	30.18	996.00	435.000	996.000	-1901	.057
2	ATP01	Attitude	Using the same password	It's safe to use the same password for social media and work accounts.	31	33.95	1052.50	34	32.13	1092.50	497.500	1092.500	-.931	.352
3	BEP01	Behavior	Using the same password	I use a different password for my social media and work accounts.	30	31.73	952.00	34	33.18	1128.00	487.000	952.000	-.572	.567
4	KNP02	Knowledge	Sharing passwords	I am allowed to share my work passwords with my colleagues.	31	33.45	1037.00	34	32.59	1108.00	513.000	1108.000	-.506	.613
5	ATP02	Attitude	Sharing passwords	It's a bad idea to share my work passwords, even if a colleague asks for it.	31	31.95	1021.50	34	33.04	1123.50	525.500	1021.500	-.066	.947
6	BEP02	Behavior	Sharing passwords	I share my work passwords with colleagues.	31	34.50	1069.50	34	31.63	1075.50	480.500	1075.500	-1.680	.093
7	KNP03	Knowledge	Using a strong password	A mixture of letters, numbers and symbols is necessary for my work passwords.	31	33.47	1037.50	33	31.59	1042.50	481.500	1042.500	-.961	.336
8	ATP03	Attitude	Using a strong password	It's safe to have a work password with just letters	31	36.45	1130.00	34	29.85	1015.00	420.000	1015.000	-2.349	.019
9	BEP03	Behavior	Using a strong password	I use a combination of letters, numbers and symbols in my work passwords.	31	35.40	1097.50	34	30.81	1047.50	452.500	1047.500	-1.635	.102

Mann Whitney U test - Email Use

					Headquarter employees			Branch employees			Test statistics			
Nr.	Code:	KAB dimension	Sub-area	Statement	N	Mean Rank	Sum of Ranks	N	Mean Rank	Sum of Ranks	Mann Whitney U	Wilcoxon W	Z	Asymp. Sig. (2-tailed)
1	KNE04	Knowledge	Clicking on links in emails (known senders)	I am allowed to click on any links in emails from people I know.	31	32.76	1015.50	34	33.22	1129.50	519.500	1015.500	-.158	.875
2	ATE04	Attitude	Clicking on links in emails (known senders)	It's always safe to click on links in emails from people I know.	31	32.40	1004.50	34	33.54	1140.50	508.500	1004.500	-.669	.504
3	BEE04	Behavior	Clicking on links in emails (known senders)	I don't always click on links in emails just because they come from someone I know.	31	33.16	1028.00	34	32.85	1117.00	522.000	1117.000	-.090	.928
4	KNE05	Knowledge	Clicking on links in emails (unknown senders)	I am not permitted to click on a link in an email from an unknown sender.	31	29.52	915.00	34	36.18	1230.00	419.000	915.000	-1.992	.046
5	ATE05	Attitude	Clicking on links in emails (unknown senders)	Nothing bad can happen if I click on a link in an email from an unknown sender.	31	33.00	1023.00	34	33.00	1122.00	527.000	1122.000	.000	1.000
6	BEE05	Behavior	Clicking on links in emails (unknown senders)	If an email from an unknown sender looks interesting, I click on a link within it.	31	35.50	1100.50	34	30.72	1044.50	449.500	1044.500	-2.205	.027
7	KNE06	Knowledge	Opening attachments in emails (unk. senders)	I am allowed to open email attachments from unknown senders.	31	30.26	938.00	34	35.50	1207.00	442.000	938.000	-2.419	.016
8	ATE06	Attitude	Opening attachments in emails (unk. senders)	It's risky to open an email attachment from an unknown sender.	31	32.90	1020.00	34	33.09	1125.00	524.000	1020.000	-.095	.925
9	BEE06	Behavior	Opening attachments in emails (unk. senders)	I don't open email attachments if the sender is unknown to me.	31	33.31	1032.50	34	32.72	1112.50	517.500	1112.500	-.209	.835

Mann Whitney U test - Social Media Use

					Headquarter employees			Branch employees			Test statistics			
Nr.	Code:	KAB dimension	Sub-area	Statement	N	Mean Rank	Sum of Ranks	N	Mean Rank	Sum of Ranks	Mann Whitney U	Wilcoxon W	Z	Asymp. Sig. (2-tailed)
1	KNS07	Knowledge	SM privacy settings	I must periodically review the privacy settings on my social media accounts.	27	32.33	873.00	33	29.00	957.00	396.000	957.000	-.942	.346
2	ATS07	Attitude	SM privacy settings	It's a good idea to regularly review my social media privacy settings.	28	34.89	977.00	34	28.71	976.00	381.000	976.000	-2.202	.028
3	BES07	Behavior	SM privacy settings	I don't regularly review my social media privacy settings.	28	35.70	999.50	33	27.02	891.50	330.500	891.500	-2.200	.028
4	KNS08	Knowledge	Considering consequences	I can't be fired for something I post on social media.	31	39.85	1235.50	34	26.75	909.50	314.500	909.500	-3.491	.000
5	ATS08	Attitude	Considering consequences	It doesn't matter if I post things on social media that I wouldn't normally say in public.	31	33.40	1035.50	34	32.63	1109.50	514.500	1109.500	-.356	.722
6	BES08	Behavior	Considering consequences	I don't post anything on social media before considering any negative consequences.	28	32.00	896.00	34	31.09	1057.00	462.000	1057.000	-.907	.364
7	KNS09	Knowledge	Posting about work	I can post what I want about work on social media.	31	33.45	1037.00	34	32.59	1108.00	513.000	1108.000	-.506	.613
8	ATS09	Attitude	Posting about work	It's risky to post certain information about my work on social media.	31	32.95	1021.50	34	33.04	1023.50	525.500	1021.500	-.066	.947
9	BES09	Behavior	Posting about work	I post whatever I want about my work on social media.	30	31.87	956.00	34	33.06	1124.00	491.000	956.000	-.698	.485

4.4.6. Contribution to ISA program design

Two research questions were formulated in order to provide an answer to our problem statement:

- What are the differences on ISA between headquarter and branch employees? (2.a)
- To what extent can the obtained insights contribute to the design of ISA programs? (2.b)

The results of the empirical part of our research provided an answer to these questions. In the previous paragraphs we have presented insight in the differences between the two employee groups. A general conclusion that could be drawn is that there are significant differences between headquarter and branch employees, which are expressed in three focus areas; password management, email use and social media use. In contrast, our test statistics also showed that no significant differences could be found within mobile devices and incident reporting. This suggests that no specific alterations have to be made in ISA programs regarding these two topics.

In the password management focus area, we observed that headquarter employees are showing higher ISA levels (paragraph 4.4.4). However, only one statement showed a significant difference between the two employee groups in favor of headquarter employees. While both employee groups know that using a strong password is part of the organizations policy, attitude regarding this matter doesn't follow. A possible explanation here is that branch employees don't agree with the measures as explained in policy, since they find it safe enough to have a work password with just letters. Convincing branch employees about the benefits of having strong passwords, as part of ISA programs, could contribute to getting support in this idea.

Regarding email use, branch employees show significantly better knowledge regarding clicking links and opening attachments in emails from unknown senders. In contrast to knowledge on this subject, headquarter employees are showing significantly better self-reported behavior. It is assumable that branch users are having more contact with unknown external parties (e.g. clients, prospects, client representatives), which accordingly might lead to clicking on links in those emails. However, this behavior is not reflected with regards to opening attachments in emails from unknown senders. If our assumption is proved correct and branch users are having email correspondence of a completely different order than headquarter employees, this should get additional focus in ISA programs for this group.

The social media use results implicate that this focus area needs special attention regarding ISA program design, especially for the branch employee user group. All three statements where differences have been found are in favor of the headquarter employees. On the knowledge statement regarding social media privacy settings, we see that the headquarter and branch employee groups are showing relatively low ISA scores (respectively 78 and 67%) but our tests did not consider this to be a significant difference. However, on the related attitude and behavior statements headquarter employees are showing significantly better awareness in favor of headquarter employees. Under the assumption that better knowledge leads to better behavior (Parsons et al., 2014), it could be beneficial to pay extra attention to this topic in ISA program design for branch users. Last but not least, respondents belonging to the branch user group have shown that they are less familiar with the possible consequences of posting content on social media. Yet, this hasn't got any influence on their self-reported behavior in this matter, where scores are (nearly) perfect. We presume that in this case knowledge of policy and procedures isn't relevant for posting on social networks.

Our conclusions are further discussed in chapter 5, where we present propositions for future research.

5. Discussion, conclusions and recommendations

5.1. Discussion – reflection

The aim of our descriptive study was to gain insight in differences between two major user groups in the banking industry (i.e. headquarter employees and branch employees), which could ultimately be beneficial for ISA program design. In their qualitative research on ISP compliance of headquarter and branch employees, Bauer et al. (2017) already argued that ISA programs should be tailored to different user groups. Their research however, does not provide insight in the actual differences between these two groups. In order to fill this gap, we have applied the R-HAIS-Q within a large bank in The Netherlands. Most banks have employees working on headquarters and branch offices and both are exposed to different IS risks (Bauer et al., 2017). Since we've observed that there are significant differences between the headquarter and branch employee groups, we support the need for tailored ISA programs which in addition to Bauer et al., (2017) has also been expressed by several other authors (Ki-Aries & Faily, 2017; McCormac et al., 2017; Wiley et al., 2020).

In order to form the R-HAIS-Q, a focus group interview has been carried out. Here, we decided to deviate from our initial plan where we intended to have an interview with the Head of Risk and an Information Security Specialist. This seemed not to be feasible from a planning perspective and on recommendation of the Head of Risk, we have performed our interview with two experts on ISA (i.e. Information Security Specialists). Luckily, this worked out to be fruitful for our research, since we were able to derive a good understanding of the contextual background and current ISA efforts of Bank X.

The R-HAIS-Q has been presented to 356 employees, where eventually 71 respondents have completed the questionnaire. A key choice we made during the creation of the R-HAIS-Q is that we incorporated a question regarding the occurrence of client contact since we explicitly stated that headquarter employees in our research don't have any client contact, while branch employees do (on a daily basis). This enabled us to increase reliability of our results, since five respondents stated to be working as headquarter employee while having daily client contact. Accordingly, these have been removed from our set of data. For one other respondent it was not possible to assign a headquarter or branch employee classification. This response has been excluded from our results, too.

Earlier, in paragraph 4.1.3, we explained that Bank X offers several ISA programs. Looking back at the process of this research, it would've been beneficial for the reliability of this study to investigate when the respondents had their last ISA intervention, and what it entailed. If we look at the size of our samples and the applied sampling technique (self-selection sampling), this implies that it is unlikely that our sample is representative for the full populations (Saunders et al., 2016). However, taking these limitations in consideration, our descriptive research has provided insight in potential differences between headquarter and branch employees, which enabled us to formulate several propositions which could be further examined in future research.

Before we proceeded with our analysis, we tested for internal reliability which resulted in excluding the knowledge dimension and several individual statements when calculating general ISA levels (paragraph 4.4.4). In contrast with other studies (Hadlington & Chivers, 2018; McCormac et al., 2016, 2017; Parsons et al., 2017, 2014; Pattinson et al., 2016; Wiley et al., 2020), where good scores for internal consistency were found, our results have shown that the knowledge dimension, as well as three focus areas (email use, social media use, mobile devices) did not meet the recommended Cronbach's alpha value (Saunders et al., 2016). This has not influenced the part of the analysis where we investigated differences on statement levels, but nevertheless, it is an unexpected finding which is in contrast with

many studies where the HAIS-Q was applied. Looking from an overall ISA perspective, including all statements, Cronbach's alpha has shown good internal consistency with a .857 Cronbach's alpha.

Our analysis has shown that there are significant differences between the headquarter and branch employee groups. Looking into more detail, we specifically observed differences in the focus areas password management, email use and social media use.

Password management – Interestingly, Bauer et al. (2017) already suggested that password management is covered better by headquarter employees than branch employees. This is in line with our results where we see a higher general level of ISA for headquarter employees, while observing a significant difference on attitude towards using strong passwords. Therefore, our first proposition is:

- P1: Attitude of branch employees towards using strong passwords is likely to be lower than those of headquarter employees.

If statistical proof is provided for this proposition it would be recommended to investigate how branch employees can be convinced of the benefits of using strong passwords, in order to gain support for this subject.

Email use – Several interesting findings are related to emails from unknown senders. Our results have shown that branch users are having significantly better knowledge of policy and procedures regarding clicking on links and opening attachments. Despite this better knowledge, they are more likely to click on links in those emails. This is a risk, since these emails could be phishing emails (Bauer et al., 2017). Having better knowledge while this doesn't lead to better behavior is in contrast with Parsons et al.'s (2014) findings. This raises the question if this result is to be considered unusual, especially when looking at both user groups' daily routine. Firstly, it is fairly possible that branch users are more interested in this topic, presumably because they are involved with unknown senders to a larger extent than their counterparts. Secondly, if branch employee's daily routine involves frequent contact with unknown parties, such as prospects or client representatives, they might feel more urge to click on links in order to handle the senders' request. We assume however that this should then also be reflected with regards to opening attachments. Lastly, headquarter employees are likely to have minimal external contact, which implicates that it's easier to step away from emails from unknown senders. A limitation of this research is that we could not validate these assumptions, since we are not aware of the extent to which the respondents have email contact with unknown parties. This brings us to the following propositions:

- P2: Branch users' knowledge regarding handling emails from unknown senders is likely to be higher than those of headquarter employees.
- P3: Branch users who have knowledge regarding clicking on links in emails from unknown senders, are unlikely to bring this knowledge into practice.
- P4: Headquarter employees are unlikely to need knowledge of clicking on links in emails from unknown users in order to practice compliant behavior.

When investigating these three propositions, we recommend dedicating special attention to the extent to which both groups have email contact with unknown senders. We deem this insight to be crucial in drawing conclusions, thus for ISA program development.

Social media use – We have found significant differences between both groups, but all are in favor of headquarter employees. Despite the fact that both user groups are not differing from each other on their knowledge regarding social media privacy settings, significant differences are found on attitude and behavior towards this subject. To benefit ISA program design, it is recommended to gain statistical evidence in this phenomenon. We have formulated the following propositions:

- P5: In contrast to headquarter employees, branch employees are likely to need knowledge of policy and procedures on social media privacy settings, in order to show increased ISA levels on attitude and behavior
- P6: In contrast to branch employees, headquarter employees are likely not to need knowledge of policy and procedures on social media privacy settings, in order to show increased ISA levels on policy and behavior.

With regards to the consideration of consequences when posting on social media (i.e. the possibility of being fired), branch users are showing significantly less knowledge than their counterparts. Despite this, our results show high ISA levels on self-reported behavior (headquarter employees 100%, branch employees 97%), which implies that it is not necessary to have knowledge of consequences in order to do the right thing.

- P7: Headquarter and branch employees do not need to know the possible consequences of posting online, since they will do the right thing anyway.

5.2. Conclusions

Several reports have shown that human behavior remains to have a large part in data breaches, which therefore is a vulnerability that should not be overlooked (Ernst & Young Global Limited, 2019; Nctv, 2019). Initiating ISA programs in order to increase an employee's ISA is an effective measure to this problem (Bauer & Bernroider, 2017; Bawazir et al., 2016). In order to increase effectiveness of these programs, they should be tailored to specific users' needs (Bauer et al., 2017; Ki-Aries & Faily, 2017; Parsons et al., 2017; Wiley et al., 2020). Banks are holding a lot of information that is valuable for malicious parties and this motivated us to perform our research in this particular context.

Two of the largest employee groups within banks are headquarter and branch employees. In their qualitative research, Bauer et al. (2017) argued that there are differences in ISA between those two groups, but what these differences comprise is unclear. Since the HAIS-Q can be used for measuring ISA (Parsons et al., 2017, 2014), we have applied (a reduced version of) this instrument on both employee groups which enabled us to gain insight in their differences. We have found differences in three focus areas; password management, email use and social media use. With regards to password management, we support Bauer et al.'s (2017) proposition that there are differences between both groups, especially regarding attitude towards using a strong password. Also, we have found significant differences related to emails from unknown senders. Our results show that having knowledge of this topic, doesn't directly lead to compliant behavior which contrasts with existing literature (Parsons et al., 2014). However, it would've been beneficial to have more information on the extent to which the respondents have contact with unknown senders. Presumably, this will occur more within the branch user group, but we do not have sufficient information to draw a conclusion on this. Significant differences were found within the social media use focus area, too. When it comes to social media privacy settings, headquarter employees showed significantly higher scores on attitude and behavior, while no significant difference was observed regarding knowledge. This implies that branch employees are likely to need knowledge in order to show higher scores on attitude and behavior, while headquarter employees don't. With regards to considering consequences when posting on social networks, we have a different insight; both groups are showing (nearly) perfect scores on self-reported behavior, however, knowledge of headquarter employees is significantly better in this matter. This might implicate that knowledge isn't needed in order to do the right thing.

Our findings have resulted in several propositions that can be further examined in future research. Ultimately, this may contribute to ISA program design, thus its effectiveness, which should result in decreasing ISP noncompliance.

5.3. Recommendations for practice

Looking at the existing body of knowledge on ISA program design in combination with our findings, we suggest that IS managers do proper investigations on ISA needs of the applicable user groups. Having a policy that is easy to access and read is a starting point, but in order to be effective, tailored ISA programs need to be set up in order to match the user's needs. To illustrate this with an example, we refer to our findings on email use. If having frequent contact with unknown parties occurs frequently, increasing awareness on this topic would be beneficial. In addition, an ISA program should not only consist of e.g. an educational e-learning, but in order to be successful, it should consist of different approaches while taking traditional and digital channels in consideration. Lastly, we have seen major differences on social media use. Our focus group interview has shown that organizations can use social media for business purposes. Therefore, it should be clear to users what is to be expected from them when it comes to these networks, in relation to personal social network accounts.

5.4. Recommendations for further research

We agree with Parsons et al. (2017) who argued that the HAIS-Q should keep up with time, and be included with e.g. focus areas related to new threats and innovative technologies. As mentioned by the Security Specialist during the focus group interview, the possibility of including questions regarding password managers (within the existing password management focus area) may be explored.

With regards to internal reliability, we have found contrasting results with existing literature. When using the HAIS-Q in future research, we recommend paying special attention to internal reliability in combination with a modular approach.

Because our research is of descriptive nature and our sampling method and size didn't enable us to draw representative conclusions, we have formulated several propositions that could be tested in quantitative studies. In the case of P2, P3 and P4 we recommend dedicating special attention to the extent to which the user groups have email contact with unknown senders.

With regards to our final recommendation, we tend to agree with Pattinson et al. (2016) who argued that employees in the financial industry are equipped with relatively high ISA. However, the financial industry involves more than only banking organizations. Future research should therefore not only focus on user perspectives within banking organizations, but also be extended towards other sectors (e.g. insurance, credit cards, investment funds etc.).

References

Allen, P., Bennett, K., & King, J. (2010). *PASW statistics by SPSS: A practical guide* (Version 18). National Library of Australia.

Bauer, S., & Bernroider, E. W. N. (2017). From information security awareness to reasoned compliant action: Analyzing information security policy compliance in a large banking organization. *Data Base for Advances in Information Systems*, *48*(3), 44–68. https://doi.org/10.1145/3130515.3130519

Bauer, S., Bernroider, E. W. N., & Chudzikowski, K. (2017). Prevention is better than cure ! Designing information security awareness programs to overcome users ' non-compliance with information security policies in banks. *Computers & Security*, *68*, 145–159. https://doi.org/10.1016/j.cose.2017.04.009

Bawazir, M. A., Mahmud, M., Molok, N. N. A., & Ibrahim, J. (2016). Persuasive Technology for Improving Information Security Awareness and Behavior: Literature Review. In *6th International Conference on Information and Communication Technology for the Muslim World*. Jakarta, Indonesia: The Institute of Electrical and Electronics Engineers, Inc. Retrieved from http://irep.iium.edu.my/55293/9/55293_Persuasive Technology for Improving Information.pdf

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, *34*(3), 523–548.

Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. H. (2015). The persuasion and security awareness experiment: reducing the success of social engineering attacks. *Journal of Experimental Criminology*, *11*(1), 97–115. https://doi.org/10.1007/s11292-014-9222-7

Christopher, L., Choo, K.-K. R., & Dehghantanha, A. (2017). *Honeypots for Employee Information Security Awareness and Education Training: A conceptual EASY training model*. (K.-K. R. Choo & A. Dehghantanha, Eds.), *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications*. Cambridge: Elsevier. https://doi.org/10.1016/b978-0-12-805303-4.00008-3

Chua, H. N., Wong, S. F., Low, Y. C., & Chang, Y. (2018). Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations. *Telematics and Informatics*, *35*(6), 1770–1780. https://doi.org/10.1016/j.tele.2018.05.005

Counotte-Potman, A., Kusters, R., & Joosten, S. (2019). *Business Process Management and IT Graduation Project Handbook* (Third). Heerlen: Open University of the Netherlands.

Da Veiga, A., & Martins, N. (2015). Information security culture and information protection culture: A validated assessment instrument. *Computer Law and Security Review*, *31*(2), 243–256. https://doi.org/10.1016/j.clsr.2015.01.005

Davison, D. B., & Chen, E. (1995). A brief introduction to the Internet. *Computers and Geosciences*, *21*(6), 731–735. https://doi.org/10.1016/0098-3004(95)00003-Q

Doorewaard, H., & Tjemkes, B. (2019). *Praktijkgericht kwantitatief onderzoek*. Boom uitgevers Amsterdam.

Ernst & Young Global Limited. (2019). EY Global Information Security Survey 2018–19. *Ey Global Information Security Survey 2018-2019*. Retrieved from https://www.ey.com/Publication/vwLUAssets/EY_Global_Information_Security_Survey_2018/$FILE/EY Global Information Security Survey 2018-19.pdf

Field, A. (2013). *Discovering statistics using IBM SPSS statistics* (4th edition). Sage.

Goldstein, J., Chernobai, A., & Benaroch, M. (2011). An Event Study Analysis of the Economic Impact of IT Operational Risk and its Subcategories An Event Study Analysis of the Economic Impact of IT Operational Risk and its Subcategories. *Journal of the Association for Information Systems*, *12*(9), 606–631.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems*, *28*(2), 203–236. https://doi.org/10.2753/MIS0742-1222280208

Hadlington, L., & Chivers, S. (2018). Segmentation Analysis of Susceptibility to Cybercrime: Exploring Individual Differences in Information Security Awareness and Personality Factors. *Policing: A Journal of Policy and Practice*, 1–14. https://doi.org/10.1093/police/pay027

Haeussinger, F. J., & Kranz, J. J. (2013). Information Security Awareness: It's Antecedents and Mediating Effects on Security Compliant Behavior. In *Thirty Fourth International Conference on Information Systems* (pp. 1–16). Milan.

Han, J. Y., Kim, Y. J., & Kim, H. (2017). An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers and Security*, *66*, 52–65. https://doi.org/10.1016/j.cose.2016.12.016

Höne, K., & Eloff, J. H. P. (2002). Information security policy - What do international information security standards say? *Computers and Security*, *21*(5), 402–409. https://doi.org/10.1016/S0167-4048(02)00504-7

Ki-Aries, D., & Faily, S. (2017). Persona-centred information security awareness. *Computers and Security*, *70*, 663–674. https://doi.org/10.1016/j.cose.2017.08.001

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers and Security*, *25*(4), 289–296. https://doi.org/10.1016/j.cose.2006.02.008

Li, Y., Spigt, R., & Swinkels, L. (2017). The impact of FinTech start-ups on incumbent retail banks' share prices. *Financial Innovation*, *3*(1). https://doi.org/10.1186/s40854-017-0076-7

Luthy, D., & Forcht, K. (2006). Laws and regulations affecting information management and frameworks for assessing compliance. *Information Management and Computer Security*, *14*(2), 155–166. https://doi.org/10.1108/09685220610655898

McCormac, A., Calic, D., Parsons, K., Zwaans, T., Butavicius, M., & Pattinson, M. (2016). Test-retest reliability and internal consistency of the human aspects of information security questionnaire (HAIS-Q). *Proceedings of the 27th Australasian Conference on Information Systems, ACIS 2016*, 1–10.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and Information Security Awareness. *Computers in Human Behavior*, *69*, 151–156. https://doi.org/10.1016/j.chb.2016.11.065

Meade, A. W., & Craig, S. B. (2012). Identifying careless responses in survey data. *Psychological Methods*, *17*(3), 437–455. https://doi.org/10.1037/a0028085

Mettouris, C., Maratou, V., Vuckovic, D., Papadopoulos, G., & Xenos, M. (2015). Information Security Awareness through a Virtual World: An end-user requirements analysis. In *International Conference on Information Society and Technology (ICIST)* (pp. 273–278).

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly: Management Information Systems*, *42*(1), 285–311. https://doi.org/10.25300/MISQ/2018/13853

Nachar, N. (2008). The Mann-Whitney U: A Test for Assessing Whether Two Independent Samples Come from the Same Distribution. *Tutorials in Quantitative Methods for Psychology*, *4*(1), 13–20. https://doi.org/10.20982/tqmp.04.1.p013

Nctv. (2019). Cybersecuritybeeld nederland. *Nctv*, 1–76. Retrieved from https://www.thehaguesecuritydelta.com/media/com_hsd/report/237/document/CSBN2019-online-tcm31-392768.pdf%0Awww.ncsc.nl

Ögütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers and Security*, *56*, 83–93. https://doi.org/10.1016/j.cose.2015.10.002

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers and Security*, *66*, 40–51. https://doi.org/10.1016/j.cose.2017.01.004

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers and Security*, *42*, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., Calic, D., & Jerram, C. (2016). The information security awareness of bank employees. In *Proceedings of the 10th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2016* (pp. 189–198).

Pattinson, Malcolm, Butavicius, M., Parsons, K., McCormac, A., & Calic, D. (2015). Factors that influence information security Behavior: An australian web-based study. In *Proceedings of human aspects of information security, privacy, & trust (HCI 2015)* (pp. 231–241). Los Angeles: Springer International Publishing.

Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research Methods for Business Students* (Seventh ed). Pearson Education Limited.

Scholl, M., Leiner, K. B., & Fuhrmann, F. (2017). Blind spot: Do you know the effectiveness of your Information security awareness-raising program? *WMSCI 2017 - 21st World Multi-Conference on Systemics, Cybernetics and Informatics, Proceedings*, *1*(4), 361–366.

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management and Computer Security*, *8*(1), 31–41. https://doi.org/10.1108/09685220010371394

Siponen, M., & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly*, *34*(3), 487–502.

Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers and Security*, *56*, 1–13. https://doi.org/10.1016/j.cose.2015.10.006

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers and Security*, *24*(2), 124–133. https://doi.org/10.1016/j.cose.2004.07.001

Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Computers and Security*, *52*, 128–141. https://doi.org/10.1016/j.cose.2015.04.006

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers and Security*, *88*. https://doi.org/10.1016/j.cose.2019.101640

World Economic Forum. (2018). *The Global Risks Report 2018*.

Yazdanmehr, A., & Wang, J. (2016). Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems*, *92*, 36–46. https://doi.org/10.1016/j.dss.2016.09.009

Appendix 1: Literature review: approach & implementation

1.1 Research approach

According to Saunders et al. (2016), literature is used for several reasons. Preliminary search helps to give insight in a research idea, a critical review gives insight in the theoretical framework and lastly, literature is used in order to discuss the research findings in relation to what is already known. As part of the complete research project, it is important to be aware of the field of research as well as the related concepts and ideas. A review helps in getting a better understanding of the topic, but critically reviewing the literature means that only relevant literature will be included. A schematic representation of the conducted critical literature review is shown in figure 6. The steps are explained as follows:

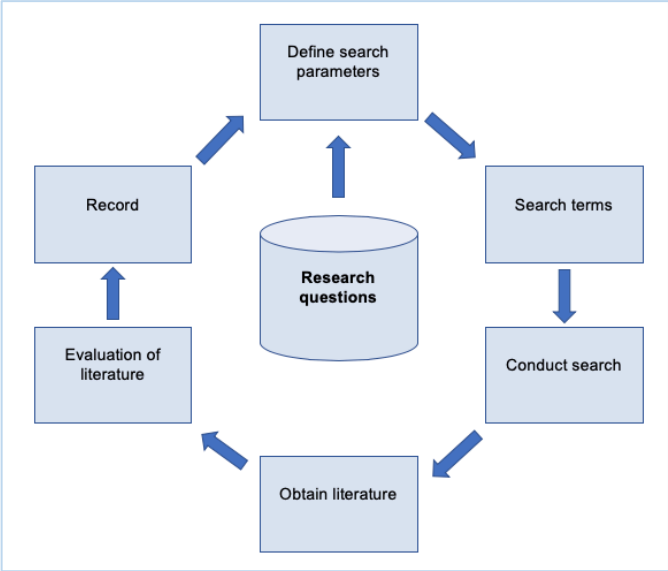

Figure 6: Schematic representation of the literature review

- *Research questions*: the research questions form the basis of the following steps.
- *Defining search parameters:* search parameters have been formulated and presented in paragraph 1.1.2 (and onwards) of this appendix.
- *Search terms*: the search terms are generated, based on the formulated research questions (paragraph 1.1.1).
- *Conduct search*: the search has been carried out in the online library of the Open University and on Google Scholar. The results of the search actions, based on the search terms, can be found in paragraph 1.2.1 of this appendix. After deduplication, the resulted list of literature is presented in paragraph 1.2.2.
- *Obtain literature*: the literature has been obtained and the documents have been stored on a local computer.
- *Evaluation of the literature*: the obtained literature has been rated on relevance and value. The results are shown in paragraph 1.2.2.
- *Record:* the obtained literature, which has been selected based on the evaluation, has provided information which has been recorded with regards to answering the research questions.

During the search, parameters and search terms have been revised and updated in order to reach literature that is more precise and relevant to answering the research questions (Saunders et al., 2016).

Regarding the approach, two sources have been used for searching literature; the Open University library and Google Scholar, and the search for literature has been conducted in three different phases:

- Search in the Open University library (journal articles)
- Search in the Open University library (conference proceedings)
- Search on Google Scholar

The phases are extensively explained in paragraphs 1.1.2 and onwards.

1.1.1 Search terms

As recommended by Saunders et al. (2016), the research questions are described in the form of identified search terms, and are mainly derived through brainstorming and initial reading of literature related to the topic. The following search terms have been derived from the research questions:

- Research question 1.a: Information security policy compliance
- Research question 1.b: Information security awareness
  Information security awareness program
  Information security awareness compliance
- Research question 1.c: Employee information security awareness
  User information security awareness
  Individual information security awareness
  Information security awareness bank

1.1.2 Search method and sources: Open University (journal articles)

This search engine (https://bibliotheek.ou.nl) searches in official publications (e.g. articles in journals, conferences, theses), in several databases and it is possible to apply parameter setting (e.g. year of publication, peer-reviewed publications, disciplines, languages etc.).

The possibility to apply parameter setting is used for filtering. The first set of parameters is applied by default, for every conducted search. In order to increase the relevance and value of the results, as well as to limit the number of results (in order to arrive at a workable amount of literature), additional parameters have been applied in a step by step approach.

Default search parameters:

- Search type: **Advanced search**
  Selecting 'advanced search' provides the opportunity to select different parameters, in contrast to 'quick search' where this is not the case.
- Language: **English**
  Selection of this parameter provided us only with articles in the English language.
- Fields: **All**
  By selecting all fields, the terms are being searched in a large variety of fields (e.g. title, author, publication title, summary, full text etc.)
- Content type: **Journal articles**
  By using this parameter, only articles from journals have been provided.
- Limit search to: **Peer-reviewed publications only**
  According to Saunders et al. (2016), peer-reviewed publications are the most useful of all since these are detailed reports of research, written by experts and evaluated by other experts, with an eye for quality.

Additional search parameters:

- Fields: **Applying Title only and Boolean logic (search strings)**
  *In order to narrow down the results, the search engine provides the opportunity to use search strings with e.g. AND, OR, *, " operators, also known as Boolean logic (Saunders et al., 2016). Also, it is possible to only search for terms in the title of an article. The final search string is presented in the implementation paragraph of this appendix (1.2).*
- Date of publication: **> 01-01-2015**
  By searching from this date, only actual articles have been provided for this literature review.
- Limit search to: **Full text online**
  By selecting this option, only articles are shown with the full text online available.
- Limit search to: **Open access items only**
  We preferably selected only publications that are freely accessible for anyone. This parameter filters all non-open access items automatically, and therefore shows only open access items.

1.1.3 Search method and source: Open University (conference proceedings)

According to Saunders et al. (2016), conference proceedings may offer information of great value to the theme of the research. Also, we didn't want to miss the opportunity to use actual, relevant information that recently has been presented on conferences. In order to retrieve relevant results, the following parameters have been applied. The default parameters were used as the start of the search, and additional parameters have been added iteratively.

Default search parameters:

- Search type: **Advanced search**
  Selecting 'advanced search' provides the opportunity to select different parameters, in contrast to 'quick search' where this is not the case.
- Language: **English**
  Selection of this parameter provided us only with articles in the English language.
- Fields: **All**
  By selecting all fields, the terms are being searched in a large variety of fields (e.g. title, author, publication title, summary, full text etc.)
- Content type: **Conference proceedings**
  By using this parameter, only conference proceedings have been provided.

Additional search parameters:

- Fields: **Applying Title only and Boolean logic (search strings)**
  *In order to narrow down the results, the search engine provides the opportunity to use search strings with e.g. AND, OR, * and*

" operators, also known as Boolean logic (Saunders et al., 2016). Also, it is possible to only search for terms in the title of an article. The final search string is presented in the implementation paragraph of this appendix (1.2).

- Date of publication: **> 01-01-2015**
  By searching from this date, only actual conference proceedings have been provided for this literature review.
- Limit search to: **Full text online**
  By selecting this option, only articles are shown with the full online text availability.
- Limit search to: **Open access items only**
  We preferably selected only publications that are freely accessible for anyone. This parameter filters all non-open access items automatically.

1.1.4 Search method and source: Google Scholar

The website of Google Scholar (https://scholar.google.com) offers a wide range of possibilities for searching literature such as e.g. articles, books and conference proceedings, from a wide range of sources such as e.g. online repositories and academic publishers. Here it is also possible to apply parameter setting, but to a rather limited extent than the Open University library. Default and additional parameters have been applied.

Default search parameters:

- Search type: **Advanced search**
  Selecting 'advanced search' provides the opportunity to select different parameters, in contrast to 'quick search' where this is not the case.
- Language: **English**
  Selection of this parameter provided us only with articles in the English language.
- Fields: **In text**
  By selecting the 'in text' parameter', the terms are being searched in the full text of the documentation.

Additional search parameters:

- Fields: **In title**
  When this parameter has been selected, only results were shown where the search terms have appeared in the title of the document.
- Date of publication: **> 2015**
  This parameter has been selected in order to retrieve recent documentation.
- Find articles: **With the exact phrase**
  By searching the search terms as an exact phrase, we only retrieved results where the search terms appeared as an exact phrase in the (title of the) document.

- Citations: **> 5**
- Citations: **> 15**

  These parameters were not available but have been manually applied in order to limit the total number of documents. This is done in order to maintain a workable amount of literature with regards to the time that is available for this research project, while focusing on relevant articles that could be examined thoroughly.

An additional manual selection took place after the selected output from Google Scholar, since parameters were available to a limited extent. Only journal articles and conference proceedings have been selected. Also, our standpoint is that only documents that are free of charge, thus freely accessible to anyone, are being selected. Since several results appeared that were not retrievable free of charge, these documents have been excluded from this research.

1.1.5 Evaluation of literature: relevance & value

By evaluation of the literature, we were able to separate the wheat from the chaff and select the articles that we found valuable and relevant to our critical review. Saunders et al. (2016) state that in assessing relevance, the obtained literature should be closely related to the research questions. Regarding value, it is important to assess the value in terms of e.g. quality (peer-reviewed articles), guidance for future research and precision (Saunders et al., 2016). We formulated the following criteria for assessment of relevance and value:

Relevance	
+	The article is closely related to the subject and provides answers to the research question(s).
+/-	The article is related to the subject. It provides answer to the research question(s) but only to a limited extent.
-	The article is not/insufficiently related to the subject and cannot contribute to the research.
Value	
+	The article is peer-reviewed, gives explicit guidance for future research and is precise in using information, dates and figures.
+/-	The article is peer-reviewed but gives limited guidance for future research and is averagely precise in information, dates and figures.
-	The article is not peer-reviewed, gives limited or no guidance for future research and is imprecise in information, dates and figures.

The rating on relevance and value, as well as a substantiation can be found in paragraph 1.2.2 of this appendix.

1.2 Implementation

Through conducting our search as described in the research approach, we obtained several academic articles which contributed to answering our research questions. But in addition, we also found relevant literature through the snowball method. In the sections below, the results with regards to the literature review are presented.

1.2.1 Search results

The search results are presented from the next page onwards.

Open University library results

Research question	Search date	Search terms	Search type	Language	Fields	Content type	Peer-reviewed publications only	Search string (Boolean logic)	Date of publication	Full text online	Open access only	# results	Output selected:
1.a	29-10-2019	Information security policy compliance	Advanced	English	All	Journal articles	Peer-reviewed publications only	(information security policy compliance)	-	-	-	100.456	
	29-10-2019	Information security policy compliance	Advanced	English	-	Journal articles	Peer-reviewed publications only	(TitleCombined:(information security policy compliance))	-	-	-	29	
	29-10-2019	Information security policy compliance	Advanced	English	-	Journal articles	Peer-reviewed publications only	(TitleCombined:(information security policy compliance))	> 01-01-2015	-	-	18	
	29-10-2019	Information security policy compliance	Advanced	English	-	Journal articles	Peer-reviewed publications only	(TitleCombined:(information security policy compliance))	> 01-01-2015	Yes	-	18	
	29-10-2019	Information security policy compliance	Advanced	English	-	Journal articles	Peer-reviewed publications only	(TitleCombined:(information security policy compliance))	> 01-01-2015	Yes	Yes	2	X
1.b	02-11-2019	Information security awareness	Advanced	English	All	Journal articles	Peer-reviewed publications only	(Information security awareness)	-	-	-	204.613	
	02-11-2019	Information security awareness	Advanced	English	-	Journal articles	Peer-reviewed publications only	(TitleCombined:(Information security awareness))	-	-	-	67	
	02-11-2019	Information security awareness	Advanced	English	-	Journal articles	Peer-reviewed publications only	(TitleCombined:(Information security awareness))	> 01-01-2015	-	-	28	
	02-11-2019	Information security awareness	Advanced	English	-	Journal articles	Peer-reviewed publications only	(TitleCombined:(Information security awareness))	> 01-01-2015	Yes	-	28	
	02-11-2019	Information security awareness	Advanced	English	-	Journal articles	Peer-reviewed publications only	(TitleCombined:(Information security awareness))	> 01-01-2015	Yes	Yes	13	
	02-11-2019	Information security awareness	Advanced	English	-	Journal articles	Peer-reviewed publications only	(TitleCombined:("Information security awareness"))	> 01-01-2015	Yes	Yes	7	X
	02-11-2019	Information security awareness program	Advanced	English	All	Journal articles	Peer-reviewed publications only	(Information security awareness program)	-	-	-	142.142	
	02-11-2019	Information security awareness program	Advanced	English	-	Journal articles	Peer-reviewed publications only	(TitleCombined:(Information security awareness program))	-	-	-	9	
	02-11-2019	Information security awareness program	Advanced	English	-	Journal articles	Peer-reviewed publications only	(TitleCombined:(Information security awareness program))	> 01-01-2015	-	-	5	
	02-11-2019	Information security awareness program	Advanced	English	-	Journal articles	Peer-reviewed publications only	(TitleCombined:(Information security awareness program))	> 01-01-2015	Yes	-	5	
	02-11-2019	Information security awareness program	Advanced	English	-	Journal articles	Peer-reviewed publications only	(TitleCombined:(Information security awareness program))	> 01-01-2015	Yes	Yes	2	X
	22-11-2019	Information security awareness compliance	Advanced	English	All	Journal articles	Peer-reviewed publications only	(Information security awareness compliance)	-	-	-	37.467	
	22-11-2019	Information security awareness compliance	Advanced	English	-	Journal articles	Peer-reviewed publications only	(TitleCombined:(information security awareness compliance))	-	-	-	4	
	22-11-2019	Information security awareness compliance	Advanced	English	-	Journal articles	Peer-reviewed publications only	(TitleCombined:(information security awareness compliance))	> 01-01-2015	-	-	3	
	22-11-2019	Information security awareness compliance	Advanced	English	-	Journal articles	Peer-reviewed publications only	(TitleCombined:(information security awareness compliance))	> 01-01-2015	Yes	-	3	X
	22-11-2019	Information security awareness compliance	Advanced	English	-	Journal articles	Peer-reviewed publications only	(TitleCombined:(information security awareness compliance))	> 01-01-2015	Yes	Yes	1	

1.c	23-11-2019	Employee information security awareness	Advanced	English	All	Journal articles	Peer-reviewed publications only	(employee security awareness)	-	-	-	51.086	
	23-11-2019	Employee information security awareness	Advanced	English	-	Journal articles	Peer-reviewed publications only	(TitleCombined:(employee security awareness))	-	-	-	2	X
	23-11-2019	Employee information security awareness	Advanced	English	-	Journal articles	Peer-reviewed publications only	(TitleCombined:(employee security awareness))	> 01-01-2015	-	-	1	
	23-11-2019	Employee information security awareness	Advanced	English	-	Journal articles	Peer-reviewed publications only	(TitleCombined:(employee security awareness))	> 01-01-2015	Yes	-	1	
	23-11-2019	Employee information security awareness	Advanced	English	-	Journal articles	Peer-reviewed publications only	(TitleCombined:(employee security awareness))	> 01-01-2015	Yes	Yes	0	
	24-11-2019	User information security awareness	Advanced	English	All	Journal articles	Peer-reviewed publications only	(User information security awareness)	-	-	-	70.136	
	24-11-2019	User information security awareness	Advanced	English	-	Journal articles	Peer-reviewed publications only	(TitleCombined:(user security awareness))	-	-	-	8	
	24-11-2019	User information security awareness	Advanced	English	-	Journal articles	Peer-reviewed publications only	(TitleCombined:(user security awareness))	> 01-01-2015	-	-	3	
	24-11-2019	User information security awareness	Advanced	English	-	Journal articles	Peer-reviewed publications only	(TitleCombined:(user security awareness))	> 01-01-2015	Yes	-	3	
	24-11-2019	User information security awareness	Advanced	English	-	Journal articles	Peer-reviewed publications only	(TitleCombined:(user security awareness))	> 01-01-2015	Yes	Yes	3	X
	24-11-2019	Individual information security awareness	Advanced	English	All	Journal articles	Peer-reviewed publications only	(individual information security awareness)	-	-	-	172.435	
	24-11-2019	Individual information security awareness	Advanced	English	-	Journal articles	Peer-reviewed publications only	(TitleCombined:(individual information security awareness))	-	-	-	3	
	24-11-2019	Individual information security awareness	Advanced	English	-	Journal articles	Peer-reviewed publications only	(TitleCombined:(individual information security awareness))	> 01-01-2015	-	-	3	
	24-11-2019	Individual information security awareness	Advanced	English	-	Journal articles	Peer-reviewed publications only	(TitleCombined:(individual information security awareness))	> 01-01-2015	Yes	-	3	X
	24-11-2019	Individual information security awareness	Advanced	English	-	Journal articles	Peer-reviewed publications only	(TitleCombined:(individual information security awareness))	> 01-01-2015	Yes	Yes	1	
	01-12-2019	Information security awareness bank	Advanced	English	All	Journal articles	Peer-reviewed publications only	(Information security awareness bank*)	-	-	-	61.999	
	01-12-2019	Information security awareness bank	Advanced	English	-	Journal articles	Peer-reviewed publications only	(TitleCombined:("Information security awareness")) AND (bank*)	-	-	-	11	
	01-12-2019	Information security awareness bank	Advanced	English	-	Journal articles	Peer-reviewed publications only	(TitleCombined:("Information security awareness")) AND (bank*)	> 01-01-2015	-	-	3	
	01-12-2019	Information security awareness bank	Advanced	English	-	Journal articles	Peer-reviewed publications only	(TitleCombined:("Information security awareness")) AND (bank*)	> 01-01-2015	Yes	-	3	X
	01-12-2019	Information security awareness bank	Advanced	English	-	Journal articles	Peer-reviewed publications only	(TitleCombined:("Information security awareness")) AND (bank*)	> 01-01-2015	Yes	Yes	1	

Open University library results (conference proceedings)

Research question	Search date	Search terms	Search type	Language	Fields	Content type	Peer-reviewed publications only	Search string (Boolean logic)	Date of publication	Full text online	Open access only	# results	Output selected:
1.a	30-11-2019	Information security policy compliance	Advanced	English	All	Conference proceedings	-	(Information security policy compliance)	-	-	-	1.675	
	30-11-2019	Information security policy compliance	Advanced	English	-	Conference proceedings	-	(TitleCombined:(Information security policy compliance))	-	-	-	5	
	30-11-2019	Information security policy compliance	Advanced	English	-	Conference proceedings	-	(TitleCombined:(Information security policy compliance))	> 01-01-2015	-	-	1	
	30-11-2019	Information security policy compliance	Advanced	English	-	Conference proceedings	-	(TitleCombined:(Information security policy compliance))	> 01-01-2015	Yes	-	1	X
	30-11-2019	Information security policy compliance	Advanced	English	-	Conference proceedings	-	(TitleCombined:(Information security policy compliance))	> 01-01-2015	Yes	Yes	0	
1.b	30-11-2019	Information security awareness	Advanced	English	All	Conference proceedings	-	(Information security awareness)	-	-	-	5.030	
	30-11-2019	Information security awareness	Advanced	English	-	Conference proceedings	-	(TitleCombined:(Information security awareness))	-	-	-	17	
	30-11-2019	Information security awareness	Advanced	English	-	Conference proceedings	-	(TitleCombined:(Information security awareness))	> 01-01-2015	-	-	3	
	30-11-2019	Information security awareness	Advanced	English	-	Conference proceedings	-	(TitleCombined:(Information security awareness))	> 01-01-2015	Yes	-	3	X
	30-11-2019	Information security awareness	Advanced	English	-	Conference proceedings	-	(TitleCombined:(Information security awareness))	> 01-01-2015	Yes	Yes	0	
	30-11-2019	Information security awareness program	Advanced	English	All	Conference proceedings	-	(Information security awareness program)	-	-	-	2.610	
	30-11-2019	Information security awareness program	Advanced	English	-	Conference proceedings	-	(TitleCombined:(Information security awareness program))	-	-	-	2	
	30-11-2019	Information security awareness program	Advanced	English	-	Conference proceedings	-	(TitleCombined:(Information security awareness program))	> 01-01-2015	-	-	0	X
	30-11-2019	Information security awareness compliance	Advanced	English	All	Conference proceedings	-	(Information security policy compliance)	-	-	-	529	
	30-11-2019	Information security awareness compliance	Advanced	English	-	Conference proceedings	-	(TitleCombined:(information security awareness compliance))	-	-	-	0	X

1.c	30-11-2019	Employee information security awareness	Advanced	English	All	Conference proceedings	-	(Employee information security awareness)	-	-	-	903		
	30-11-2019	Employee information security awareness	Advanced	English	-	Conference proceedings	-	(TitleCombined:(Employee information security awareness))	-	-	-	1		
	30-11-2019	Employee information security awareness	Advanced	English	-	Conference proceedings	-	(TitleCombined:(Employee information security awareness))	> 01-01-2015	-	-	0	X	
	30-11-2019	User information security awareness	Advanced	English	All	Conference proceedings	-	(User information security awareness)	-	-	-	4.125		
	30-11-2019	User information security awareness	Advanced	English	-	Conference proceedings	-	(TitleCombined:(User information security awareness))	-	-	-	2	X	
	30-11-2019	User information security awareness	Advanced	English	-	Conference proceedings	-	(TitleCombined:(User information security awareness))	> 01-01-2015	-	-	1		
	30-11-2019	User information security awareness	Advanced	English	-	Conference proceedings	-	(TitleCombined:(User information security awareness))	> 01-01-2015	Yes	-	1		
	30-11-2019	User information security awareness	Advanced	English	-	Conference proceedings	-	(TitleCombined:(User information security awareness))	> 01-01-2015	Yes	Yes	0		
	30-11-2019	Individual information security awareness	Advanced	English	All	Conference proceedings	-	(individual information security awareness)	-	-	-	3.130		
	30-11-2019	Individual information security awareness	Advanced	English	-	Conference proceedings	-	(TitleCombined:(individual information security awareness))	-	-	-	0	X	
	01-12-2019	Information security awareness bank	Advanced	English	All	Conference proceedings	-	(Information security awareness bank*)	-	-	-	792		
	01-12-2019	Information security awareness bank	Advanced	English	-	Conference proceedings	-	(TitleCombined:(Information security awareness)) AND (bank*)	-	-	-	0	X	

Google Scholar results

Research question	Search date	Search terms	Search type	Language	Search terms	Date of publication	With the exact phrase	Search string	Citations >5	Citations >15	# results	Output selected:
1.a	29-11-2019	Information security policy compliance	Advanced	English	In text	-	-	Information security policy compliance	-	-	1.600.000	
	29-11-2019	Information security policy compliance	Advanced	English	In title	-	-	allintitle: Information security policy compliance	-	-	134	
	29-11-2019	Information security policy compliance	Advanced	English	In title	> 2015	-	allintitle: Information security policy compliance	-	-	81	
	29-11-2019	Information security policy compliance	Advanced	English	In title	> 2015	Yes	allintitle: "Information security policy compliance"	-	-	74	
	29-11-2019	Information security policy compliance	Advanced	English	In title	> 2015	Yes	allintitle: "Information security policy compliance"	Yes	-	16	
	29-11-2019	Information security policy compliance	Advanced	English	In title	> 2015	Yes	allintitle: "Information security policy compliance"	-	Yes	6	X
1.b	01-12-2019	Information security awareness	Advanced	English	In text	-	-	Information security awareness	-	-	3.000.000	
	01-12-2019	Information security awareness	Advanced	English	In title	-	-	allintitle: Information security awareness	-	-	569	
	01-12-2019	Information security awareness	Advanced	English	In title	> 2015	-	allintitle: Information security awareness	-	-	250	
	01-12-2019	Information security awareness	Advanced	English	In title	> 2015	Yes	allintitle: "Information security awareness"	-	-	207	
	01-12-2019	Information security awareness	Advanced	English	In title	> 2015	Yes	allintitle: "Information security awareness"	Yes	-	35	
	01-12-2019	Information security awareness	Advanced	English	In title	> 2015	Yes	allintitle: "Information security awareness"	-	Yes	12	X
	29-11-2019	Information security awareness program	Advanced	English	In text	-	-	Information security awareness program	-	-	1.730.000	
	29-11-2019	Information security awareness program	Advanced	English	In title	-	-	allintitle: Information security awareness program	-	-	32	
	29-11-2019	Information security awareness program	Advanced	English	In title	> 2015	-	allintitle: Information security awareness program	-	-	12	
	29-11-2019	Information security awareness program	Advanced	English	In title	> 2015	Yes	allintitle: "Information security awareness program"	-	-	7	
	29-11-2019	Information security awareness program	Advanced	English	In title	> 2015	Yes	allintitle: "Information security awareness program"	Yes	-	2	X
	29-11-2019	Information security awareness program	Advanced	English	In title	> 2015	Yes	allintitle: "Information security awareness program"	-	Yes	0	
	29-11-2019	Information security awareness compliance	Advanced	English	In text	-	-	Information security awareness compliance	-	-	511.000	
	29-11-2019	Information security awareness compliance	Advanced	English	In title	-	-	allintitle: Information security awareness compliance	-	-	18	
	29-11-2019	Information security awareness compliance	Advanced	English	In title	> 2015	-	allintitle: Information security awareness compliance	-	-	11	
	29-11-2019	Information security awareness compliance	Advanced	English	In title	> 2015	Yes	allintitle: "Information security awareness compliance"	-	-	0	
	29-11-2019	Information security awareness compliance	Advanced	English	In title	> 2015	-	allintitle: Information security awareness compliance	Yes	-	4	X
	29-11-2019	Information security awareness compliance	Advanced	English	In title	> 2015	-	allintitle: Information security awareness compliance	-	Yes	3	

1.c	29-11-2019	Employee information security awareness	Advanced	English	In text	-	-	Employee information security awareness	-	-	565.000		
	29-11-2019	Employee information security awareness	Advanced	English	In title	-	-	allintitle: Employee information security awareness	-	-	13		
	29-11-2019	Employee information security awareness	Advanced	English	In title	> 2015	-	allintitle: Employee information security awareness	-	-	10		
	29-11-2019	Employee information security awareness	Advanced	English	In title	> 2015	Yes	allintitle: "Employee information security awareness"	-	-	5		
	29-11-2019	Employee information security awareness	Advanced	English	In title	> 2015	Yes	allintitle: "Employee information security awareness"	Yes	-	1	X	
	29-11-2019	Employee information security awareness	Advanced	English	In title	> 2015	Yes	allintitle: "Employee information security awareness"	-	Yes	0		
	29-11-2019	User information security awareness	Advanced	English	In text	-	-	User information security awareness	-	-	1.030.000		
	29-11-2019	User information security awareness	Advanced	English	In title	-	-	allintitle: User information security awareness	-	-	20		
	29-11-2019	User information security awareness	Advanced	English	In title	> 2015	-	allintitle: User information security awareness	-	-	9		
	29-11-2019	User information security awareness	Advanced	English	In title	> 2015	Yes	allintitle: "User information security awareness"	-	-	0		
	29-11-2019	User information security awareness	Advanced	English	In title	> 2015	-	allintitle: User information security awareness	Yes	-	3	X	
	29-11-2019	User information security awareness	Advanced	English	In title	> 2015	-	allintitle: User information security awareness	-	Yes	1		
	29-11-2019	Individual information security awareness	Advanced	English	In text	-	-	Individual information security awareness	-	-	2.020.000		
	29-11-2019	Individual information security awareness	Advanced	English	In title	-	-	allintitle: Individual information security awareness	-	-	5		
	29-11-2019	Individual information security awareness	Advanced	English	In title	> 2015	-	allintitle: Individual information security awareness	-	-	5		
	29-11-2019	Individual information security awareness	Advanced	English	In title	> 2015	Yes	allintitle: "Individual information security awareness"	-	-	1		
	29-11-2019	Individual information security awareness	Advanced	English	In title	> 2015	-	allintitle: Individual information security awareness	Yes	-	2		
	29-11-2019	Individual information security awareness	Advanced	English	In title	> 2015	-	allintitle: Individual information security awareness	-	Yes	2	X	
	01-12-2019	Information security awareness bank	Advanced	English	In text	-	-	Information security awareness bank*	-	-	844.000		
	01-12-2019	Information security awareness bank	Advanced	English	In title	-	-	allintitle: Information security awareness bank	-	-	6		
	01-12-2019	Information security awareness bank	Advanced	English	In title	> 2015	-	allintitle: Information security awareness bank	-	-	6	X	
	01-12-2019	Information security awareness bank	Advanced	English	In title	> 2015	Yes	allintitle: "Information security awareness bank"	-	-	1		
	01-12-2019	Information security awareness bank	Advanced	English	In title	> 2015	Yes	allintitle: "Information security awareness bank"	Yes	-	0		
	01-12-2019	Information security awareness bank	Advanced	English	In title	> 2015	Yes	allintitle: "Information security awareness bank"	-	Yes	0		

1.2.2 Overview, assessment and selection of literature

The literature that was obtained through the search actions is presented per research question, from the next page onwards. The articles have been rated on relevance and value, with a substantiation and the applicable APA reference. Please note that results (documents) sometimes appeared in other search actions as well. Therefore, deduplication has been applied and the results are therefore showing unique articles per research question.

Search results Open University Library (journal articles)

How is an ISP formed and what is ISP compliance? (1.a)

Article number	Title	Relevance	Value	Selected (Y/N)	Explanation	APA reference
1.	Information security policy compliance model in organisations	+	+/-	Y	This article contributes to this research by providing answers to one or more research questions. Nevertheless, precision is average, the scope is very broad and there is no relation to banking.	Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly, 34*(3), 523–548.
2.	Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks	+	+	Y	This article is relevant in providing answers to one or more research questions. There is explicit guidance for further research, and the scope is limited to banking.	Bauer, S., Bernroider, E. W. N., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users ' non-compliance with information security policies in banks. *Computers & Security, 68*, 145–159. https://doi.org/10.1016/j.cose.2017.04.009

What is ISA and how can the design of an ISA program contribute to increasing ISA? (1.b)

Article number	Title	Relevance	Value	Selected (Y/N)	Explanation	APA reference
3.	Persona-centred information security awareness	+/-	+/-	Y	This article provides a limited contribution to one or more research questions, since the authors investigated the incorporation of personas in ISA design and implementation. Information is presented averagely precise. The literature used comes primarily from textbooks, conferences and tech reports; no peer-reviewed articles have been used. Recommendations for further research are rather limited.	Ki-Aries, D., & Faily, S. (2017). Persona-centred information security awareness. *Computers and Security, 70*, 663–674. https://doi.org/10.1016/j.cose.2017.08.001
4.	A Reliable Measure of Information Security Awareness and the Identification of Bias in Responses	+	+	Y	This article provides input for answering one or more research questions, since it evaluates the reliability of the HAIS-Q measuring method for ISA.	McCormac, A., Calic, D., Butavicius, M., Parsons, K., Zwaans, T., & Pattinson, M. (2017). A reliable measure of information security awareness and the identification of bias in responses. *Australasian Journal of Information Systems, 21* doi:10.3127/ajis.v21i0.1697
-	The information security awareness of the Slovakian kindergarten teacher students at starting and finishing the study in higher education	-	+	N	This article does not contribute to answering the research questions. The scope of the research is limited to kindergartens. Obtained insights have been presented precisely.	Kiss, G. (2019). The information security awareness of the slovakian kindergarten teacher students at starting and finishing the study in higher education. *SHS Web of Conferences, 66*, 1042. doi:10.1051/shsconf/20196601042

5.	Blind Spot: Do You Know the Effectiveness of Your Information Security Awareness-Raising Program?	+	+/-	Y	This peer-reviewed article provides input for answering one or more research questions, since the authors investigated several measuring methods on effectiveness. Nevertheless, precision is average.	Scholl, M., Leiner, K. B., & Fuhrmann, F. (2017). Blind spot: Do you know the effectiveness of your Information security awareness-raising program? *WMSCI 2017 - 21st World Multi-Conference on Systemics, Cybernetics and Informatics, Proceedings, 1*(4), 361–366.
6.	Segmentation Analysis of Susceptibility to Cybercrime: Exploring Individual Differences in Information Security Awareness and Personality Factors	+/-	+	Y	A limited answer has been provided to the research questions in this peer-reviewed paper. Information is precise and future directions for research have been provided.	Hadlington, L., & Chivers, S. (2018). Segmentation Analysis of Susceptibility to Cybercrime: Exploring Individual Differences in Information Security Awareness and Personality Factors. *Policing: A Journal of Policy and Practice*, 1–14. https://doi.org/10.1093/police/pay027
-	An investigation into users' information security awareness on social networks in south western Nigeria	-	+/-	N	This article does not provide input for answering the research questions, since it investigates ISA amongst individuals regarding social networking. Information is limited, and results are not relevant for this study.	Okesola, J. O., Onashoga, A., & Ogunbanwo, A. (2016). An investigation into users' information security awareness on social networks in south western nigeria. *SA Journal of Information Management, 18*(1), e1-e7. doi:10.4102/sajim.v18i1.721
7.	Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations	+	+	Y	This article contributes to answering one or more research questions.	Chua, H. N., Wong, S. F., Low, Y. C., & Chang, Y. (2018). Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations. *Telematics and Informatics, 35*(6), 1770-1780. doi:10.1016/j.tele.2018.05.005

How can users' ISA be measured? (1.c)

Article number	Title	Relevance	Value	Selected (Y/N)	Explanation	APA reference
8.	Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)	+	+	Y	The article provided information and a methodology about how measurement of ISA amongst employees can be conducted. It is a detailed representation of their research which gives sufficient further directions for future research.	Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & Security, 42*, 165-176. doi:10.1016/j.cose.2013.12.003
-	Information disclosure of social media users: Does control over personal information, user awareness and security notices matter?	-	+/-	N	The article is focused on users in the context of social networks. Therefore, their findings cannot contribute to our research. Information is detailed and precise, but recommendations for further research have not been given clearly.	Benson, V., Saridakis, G., & Tennakoon, H. (2015). Information disclosure of social media users does control over personal information, user awareness and security notices matter? *Information Technology & People, 28*(3), 426-441. doi:10.1108/ITP-10-2014-0232
9.	Individual differences and Information Security Awareness	+	+	Y	The article, which gives insight in the relations between individual differences and ISA, provided answers to the research questions. Information is detailed and a clearly presented and guidance for future research has been provided.	McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior, 69*, 151-156. doi:10.1016/j.chb.2016.11.065
10.	More than the individual: Examining the relationship between culture and Information Security Awareness	+	+	Y	The article provided answers to the research questions, since individual differences have been measured with regards to ISA. Recommendations for further research have been given and information and details are presented in a precise matter.	Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and information security awareness. *Computers & Security, 88*, 101640. doi:10.1016/j.cose.2019.101640
-	A Cross Industry Study of Institutional Pressures on Organizational Effort to Raise Information Security Awareness	-	+/-	N	The article does not provide an answer to (one of the) research questions. Precision is high regarding details and information, and adequate options for further research have been provided.	Kam, H. J., Mattson, T., & Goel, S. (2019). A Cross Industry Study of Institutional Pressures on Organizational Effort to Raise Information Security Awareness. *Information Systems Frontiers,* 1-24.

Search results Open University Library (conference proceedings)

How is an ISP formed and what is ISP compliance? (1.a)

Article number	Title	Relevance	Value	Selected (Y/N)	Explanation	APA reference
-	Ambiguity as a Barrier to Information Security Policy Compliance: A Content Analysis	X	X	N	Document not available free of charge .	Buthelezi, M. P., Van Der Poll, J. A., & Ochola, E. O. (2016, December). Ambiguity as a barrier to information security policy compliance: A content analysis. In *2016 International Conference on Computational Science and Computational Intelligence (CSCI)* (pp. 1360-1367). IEEE.

What is ISA and how can the design of an ISA program contribute to increasing ISA? (1.b)

Article number	Title	Relevance	Value	Selected (Y/N)	Explanation	APA reference
11.	Persuasive Technology for Improving Information Security Awareness and Behavior: Literature Review	+	+	Y	The document provides insight in using persuasive technology for improving information security awareness. Information is quite precise, but no recommendations for further research have been provided.	Bawazir, M. A., Mahmud, M., Molok, N. N. A., & Ibrahim, J. (2016). Persuasive Technology for Improving Information Security Awareness and Behavior: Literature Review. In *6th International Conference on Information and Communication Technology for the Muslim World*. Jakarta, Indonesia: The Institute of Electrical and Electronics Engineers, Inc. Retrieved from http://irep.iium.edu.my/55293/9/55293_Persuasive Technology for Improving Information.pdf
-	Analysis of Awareness Structures in Information Security Systems	X	X	N	Document not available free of charge.	Styugin, M. (2015, October). Analysis of Awareness Structures in Information Security Systems. In *2015 Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec)* (pp. 6-10). IEEE.
-	Evaluation of Users' Awareness and Their Reaction on Information Security	X	X	N	Document not available free of charge.	Zeki, A. M., & Hamid, H. (2015, December). Evaluation of Users' Awareness and Their Reaction on Information Security. In *2015 4th International Conference on Advanced Computer Science Applications and Technologies (ACSAT)* (pp. 251-255). IEEE.

How can users' ISA be measured? (1.c)

Article number	Title	Relevance	Value	Selected (Y/N)	Explanation	APA reference
-	Users' Awareness of and Perception on Information SecurityIssues: A Case Study of Kulliyyah of ICT Postgraduate Students	X	X	N	Document not available free of charge.	Hamid, H., & Zeki, A. M. (2014, December). Users' Awareness of and Perception on Information Security Issues: A Case Study of Kulliyyah of ICT Postgraduate Students. In *2014 3rd International Conference on Advanced Computer Science Applications and Technologies* (pp. 139-144). IEEE.

Search results Google Scholar

How is an ISP formed and what is ISP compliance? (1.a)

Article number	Title	Relevance	Value	Selected (Y/N)	Explanation	APA reference
12.	Toward a unified model of information security policy compliance	+/-	+	Y	The article focusses on comparing several IS behavior models and creating one unified model, which would not directly contribute to our research. Nevertheless, a definition of ISP compliance was provided and therefore it contributes to answering a research question to a limited extent. Value is positively rated because of precise information and clear propositions for further research. Also, the article is peer-reviewed.	Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly: Management Information Systems, 42*(1), 285–311. https://doi.org/10.25300/MISQ/2018/13853
13.	Employees' information security policy compliance: A norm activation perspective	+/-	+/-	Y	This paper provided answer to a research question to a limited extent. Information is precise but directions for futher research are not very detailed.	Yazdanmehr, A., & Wang, J. (2016). Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems, 92*, 36-46.
14.	From Information Security Awareness to Reasoned Compliant Action: Analyzing Information Security Policy Compliance in a Large Banking Organization	+	+	Y	Provided input on why an ISP is formed, and the design of ISA programs. Therefore, it contributes to answering one or more research questions. It's a peer-reviewed paper and information is precise.	Bauer, S., & Bernroider, E. W. (2017). From information security awareness to reasoned compliant action: analyzing information security policy compliance in a large banking organization. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 48*(3), 44-68.
15.	An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective	+/-	+	Y	The article contributed to providing an answer to a research question, but to a limited extent. Value is good since it's peer-reviewed, very precise and clear further research directions have been given.	Han, J., Kim, Y. J., & Kim, H. (2017). An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers & Security, 66,* 52-65.

What is ISA and how can the design of an ISA program contribute to increasing ISA? (1.b)

Article number	Title	Relevance	Value	Selected (Y/N)	Explanation	APA reference
16.	Analysis of personal information security behavior and awareness	+/-	+/-	Y	The paper contributed to answering a research question to a limited extent (age and education regarding ISA). Directions for further research are limited, but details are precise, and the article has been peer-reviewed.	Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security, 56*, 83-93.
17.	Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs	+/-	+/-	Y	The paper provided a limited answer to one research question. It contributed with regards to ISA and individual differences. The article is peer-reviewed and is averagely precise. Directions for further research are limited.	Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Computers & security, 52*, 128-141.

-	Leadership styles and information security compliance behavior: The mediator effect of information security awareness	-	+	N	The article does not provide answer to the research questions. It focusses on leadership and is primarily interesting for the medical sector. It's a peer-reviewed publication with precise information, but future directions are limited.	Humaidi, N., & Balakrishnan, V. (2015). Leadership styles and information security compliance behavior: The mediator effect of information security awareness. *International Journal of Information and Education Technology, 5*(4), 311.
-	Information security awareness at the knowledge-based institution: its antecedents and measures	-	-	N	The article does not answer one or more of the research questions. Information is precise, but the use of the English language is mediocre. No directions for further research have been provided.	Ahlan, A. R., Lubis, M., & Lubis, A. R. (2015). Information security awareness at the knowledge-based institution: its antecedents and measures. *Procedia Computer Science, 72*, 361-373.

How can users' ISA be measured? (1.c)

Article number	Title	Relevance	Value	Selected (Y/N)	Explanation	APA reference
18.	Honeypots for employee information security awareness and education training: a conceptual EASY training model	+/-	+/-	Y	The article provided limited answer to one of the research questions.	Christopher, L., Choo, K. K., & Dehghantanha, A. (2017). Honeypots for employee information security awareness and education training: a conceptual EASY training model. In *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications* (pp. 111-129). Syngress.
19.	Information Security Awareness through a Virtual World: An end-user requirements analysis	+/-	+/-	Y	The authors argue that a 3D virtual world can be used as a learning environment for ISA. It therefore gives a limited answer to one of the research questions. No directions for further research have been provided.	Mettouris, C., Maratou, V., Vuckovic, D., Papadopoulos, G. A., & Xenos, M. (2015). Information Security Awareness through a Virtual World: An end-user requirements analysis. In *5th International Conference on Information Society and Technology, ICIST2015* (pp. 273-278).
20.	The information security awareness of bank employees	+	+/-	Y	The paper provided answer to the research question regarding measuring ISA in the banking industry. Information is detailed, but no directions for further research have been provided.	Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., Calic, D., & Jerram, C. (2016). The information security awareness of bank employees. In *Proceedings of the 10th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2016* (pp. 189–198).
-	Building an Information Security Awareness Program for a Bank: Case from Ethiopia	-	-	N	The paper is providing an ISA program for a specified bank in Ethiopia (practical research) and is therefore not filling a gap in academic literature. Precision is mediocre and limited directions for further research have been provided.	Bogale, M., Lessa, L., & Negash, S. (2019). Building an information security awareness program for a bank: Case from Ethiopia. *25th Americas Conference on Information Systems, AMCIS 2019*, 1–10.

1.2.3 Snowball method

While reading relevant articles that evolved from the search actions, we also found literature through the bibliography of those articles. This way of finding literature is referred to as the 'snowball method'.

Article number	Derived from article number	Title	Explanation	APA reference
1.1.	1.	From information security to cyber security	The article provided input regarding differences between information security and cyber security.	Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security, 38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004
2.1.	2.	Laws and regulations affecting information management and frameworks for assessing compliance	From this article, input regarding the Basel II Accord was derived.	Luthy, D., & Forcht, K. (2006). Laws and regulations affecting information management and frameworks for assessing compliance. *Information Management and Computer Security, 14*(2), 155–166. https://doi.org/10.1108/09685220610655898
2.2.	2.	Information security policy – what do international information security standards say?	The paper provided input regarding how ISP's are formed.	Höne, K., & Eloff, J. H. P. (2002). Information security policy - What do international information security standards say? *Computers and Security, 21*(5), 402–409. https://doi.org/10.1016/S0167-4048(02)00504-7
2.3	2.	The persuasion and security awareness experiment: reducing the success of social engineering attacks	The paper provided a method for measuring ISP compliance.	Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. H. (2015). The persuasion and security awareness experiment: reducing the success of social engineering attacks. *Journal of Experimental Criminology, 11*(1), 97–115. https://doi.org/10.1007/s11292-014-9222-7
4.1	4.	A conceptual foundation for organizational information security awareness	A definition of ISA was provided by this article.	Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management and Computer Security, 8*(1), 31–41. https://doi.org/10.1108/09685220010371394
6.1	6.	Analysis of end user security behaviors	The article consists of a survey regarding password management, thus provided answer to how a focus area within ISA could be measured.	Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers and Security, 24*(2), 124–133. https://doi.org/10.1016/j.cose.2004.07.001
7.1	7.	Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations	The paper provided information regarding noncompliance with ISP's.	Siponen, M., & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly, 34*(3), 487–502.

8.1	8.	A prototype for assessing information security awareness	The paper provided information regarding the assessment of ISA among employees.	Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers and Security, 25*(4), 289–296. https://doi.org/10.1016/j.cose.2006.02.008
9.1	9.	Factors that influence information security Behavior: An Australian web-based study	The results of the study showed proof of age being of influence on ISA scores.	Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., & Calic, D. (2015). Factors that influence information security Behavior: An australian web-based study. In *Human Aspects of Information Security, Privacy, and Trust* (pp. 231–241). Springer International Publishing.
10.1	10.	The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies	The paper provided information regarding the HAIS-Q.	Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers and Security, 66*, 40–51. https://doi.org/10.1016/j.cose.2017.01.004
10.2	10.	Information security culture and information protection culture: A validated assessment instrument	The paper provided insight in the topic of security culture.	Da Veiga, A., & Martins, N. (2015). Information security culture and information protection culture: A validated assessment instrument. *Computer Law and Security Review, 31*(2), 243–256. https://doi.org/10.1016/j.clsr.2015.01.005
10.3	10.	Test-retest reliability and internal consistency of the human aspects of information security questionnaire (HAIS-Q)	The paper provided insight in reliability and validity of the HAIS-Q.	McCormac, A., Calic, D., Parsons, K., Zwaans, T., Butavicius, M., & Pattinson, M. (2016). Test-retest reliability and internal consistency of the human aspects of information security questionnaire (HAIS-Q). *Proceedings of the 27th Australasian Conference on Information Systems, ACIS 2016*, 1–10.
14.1	14.	Understanding Nonmalicious Security Violations in the Workplace: A Composite behavior model	Input was provided regarding actions that lead to ISP non-compliance.	Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems, 28*(2), 203–236. https://doi.org/10.2753/MIS0742-1222280208
17.1	17.	Information Security Awareness: It's Antecedents and Mediating Effects on Security Compliant Behavior.	The article provided information regarding the effectiveness of information security awareness on ISP compliance.	Haeussinger, F. J., & Kranz, J. J. (2013). Information Security Awareness: It's Antecedents and Mediating Effects on Security Compliant Behavior. In *Thirty Fourth International Conference on Information Systems* (pp. 1–16). Milan.

Appendix 2: HAIS-Q

Table 9: HAIS-Q of Parsons et al., (2017)

	Knowledge	Attitude	Behaviour
Focus area: Password management			
Using the same password	It's acceptable to use my social media passwords on my work accounts. ^	It's safe to use the same password for social media and work accounts. ^	I use a different password for my social media and work accounts.
Sharing passwords	I am allowed to share my work passwords with colleagues. ^	It's a bad idea to share my work passwords, even if a colleague asks for it.	I share my work passwords with colleagues. ^
Using a strong password	A mixture of letters, numbers and symbols is necessary for work passwords.	It's safe to have a work password with just letters. ^	I use a combination of letters, numbers and symbols in my work passwords.
Focus area: Email use			
Clicking on links in emails from known senders	I am allowed to click on any links in emails from people I know. ^	It's always safe to click on links in emails from people I know. ^	I don't always click on links in emails just because they come from someone I know.
Clicking on links in emails from unknown senders	I am not permitted to click on a link in an email from an unknown sender.	Nothing bad can happen if I click on a link in an email from an unknown sender. ^	If an email from an unknown sender looks interesting, I click on a link within it. ^
Opening attachments in emails from unknown senders	I am allowed to open email attachments from unknown senders. ^	It's risky to open an email attachment from an unknown sender.	I don't open email attachments if the sender is unknown to me.
Focus area: Internet use			
Downloading files	I am allowed to download any files onto my work computer if they help me to do my job. ^	It can be risky to download files on my work computer.	I download any files onto my work computer that will help me get the job done. ^
Accessing dubious websites	While I am at work, I shouldn't access certain websites.	Just because I can access a website at work, doesn't mean that it's safe.	When accessing the Internet at work, I visit any website that I want to. ^
Entering information online	I am allowed to enter any information on any website if it helps me do my job. ^	If it helps me to do my job, it doesn't matter what information I put on a website. ^	I assess the safety of websites before entering information.
Focus area: Social media use			
SM privacy settings	I must periodically review the privacy settings on my social media accounts.	It's a good idea to regularly review my social media privacy settings.	I don't regularly review my social media privacy settings. ^
Considering consequences	I can't be fired for something I post on social media. ^	It doesn't matter if I post things on social media that I wouldn't normally say in public. ^	I don't post anything on social media before considering any negative consequences.
Posting about work	I can post what I want about work on social media. ^	It's risky to post certain information about my work on social media.	I post whatever I want about my work on social media. ^
Focus area: Mobile devices			
Physically securing mobile devices	When working in a public place, I have to keep my laptop with me at all times.	When working in a café, it's safe to leave my laptop unattended for a minute. ^	When working in a public place, I leave my laptop unattended. ^
Sending sensitive information via Wi-Fi	I am allowed to send sensitive work files via a public Wi-Fi network. ^	It's risky to send sensitive work files using a public Wi-Fi network.	I send sensitive work files using a public Wi-Fi network. ^
Shoulder surfing	When working on a sensitive document, I must ensure that strangers can't see my laptop screen.	It's risky to access sensitive work files on a laptop if strangers can see my screen.	I check that strangers can't see my laptop screen if I'm working on a sensitive document.
Focus area: Information handling			
Disposing of sensitive print-outs	Sensitive print-outs can be disposed of in the same way as non-sensitive ones.^	Disposing of sensitive print-outs by putting them in the rubbish bin is safe. ^	When sensitive print-outs need to be disposed of, I ensure that they are shredded or destroyed.
Inserting removable media	If I find a USB stick in a public place, I shouldn't plug it into my work computer.	If I find a USB stick in a public place, nothing bad can happen if I plug it into my work computer. ^	I wouldn't plug a USB stick found in a public place into my work computer.
Leaving sensitive material	I am allowed to leave print-outs containing sensitive information on my desk overnight. ^	It's risky to leave print-outs that contain sensitive information on my desk overnight.	I leave print-outs that contain sensitive information on my desk when I'm not there. ^
Focus area: Incident reporting			
Reporting suspicious behaviour	If I see someone acting suspiciously in my workplace, I should report it.	If I ignore someone acting suspiciously in my workplace, nothing bad can happen. ^	If I saw someone acting suspiciously in my workplace, I would do something about it.
Ignoring poor security behaviour by colleagues	I must not ignore poor security behaviour by my colleagues.	Nothing bad can happen if I ignore poor security behaviour by a colleague. ^	If I noticed my colleague ignoring security rules, I wouldn't take any action. ^
Reporting all incidents	It's optional to report security incidents. ^	It's risky to ignore security incidents, even if I think they're not significant.	If I noticed a security incident, I would report it.

Note. Participants are instructed to respond to each item on a five-point scale from "Strongly Disagree" to "Strongly Agree".
^ Reverse scoring was used on this item.

Appendix 3: Information sheet

Beste heer/mevrouw ***,

Graag wil ik u uitnodigen voor een interview ten behoeve van mijn afstudeeronderzoek van de Masteropleiding Business Process Management & IT.

Mijn onderzoek richt zich op information security awareness (ISA). Omdat uit literatuur blijkt dat er veel verschillen bestaan m.b.t. kennis, houding en gedrag van personen op het gebied van ISA, doe ik hier verder onderzoek naar. Ik richt mij in mijn onderzoek op het beschrijven van verschillen tussen twee verschillende gebruikersgroepen, te weten; hoofdkantoormedewerkers (specifiek: geen klantcontact) en lokale bankmedewerkers (specifiek: dagelijks klantcontact). Het doel is om ISA van deze groepen te vergelijken, verschillen te herkennen en proposities voor te stellen die uiteindelijk (in vervolgonderzoek) statistisch getoetst kunnen worden. De resultaten kunnen worden gebruikt voor het verbeteren van security awareness programma's.

Om de verschillen tussen de groepen te onderzoeken wil ik een enquête uitzetten onder de betreffende medewerkersgroepen. Het gaat hier om de Human Aspects of Information Security Questionnaire (HAIS-Q), waarbij wetenschappelijk is vastgesteld dat deze een juist beeld geeft van awareness onder de respondenten. De vragenlijst is modulair ingericht en kan daarom worden verkort in samenspraak met de organisatie waar deze wordt uitgezet. Een kortere vragenlijst heeft de voorkeur, omdat de lengte van de originele HAIS-Q mogelijk kan leiden tot ontmoediging bij de respondenten. Het doel van het interview is daarom om;

- Achtergrondinformatie te verkrijgen m.b.t. de huidige security awareness situatie (en programma's) bij uw organisatie;
- Tot een uiteindelijke selectie van vragen/onderwerpen uit de HAIS-Q te komen die voorgelegd kunnen worden aan de respondenten.

Conform mijn afstudeervoorstel zou ik graag een groepsinterview willen doen met u beiden, gezien uw specialistische rol met betrekking tot dit onderwerp. Tijdens het interview zal een voice-recorder worden gebruikt ten behoeve van nadere uitwerking en analyse. Uiteraard vindt het interview alleen plaats op vrijwillige basis, en u behoudt het recht om vragen niet te beantwoorden. Daarbij kunt u zich te allen tijde terugtrekken uit het interview. Het uiteindelijke rapport wordt openbaar gepubliceerd, echter worden alle gegevens (waar nodig) volledig geanonimiseerd. Daarbij wordt ruwe data (nadat deze is geanonimiseerd) bewaard op een beveiligde, lokale drager. Indien er vragen zijn met betrekking tot het uitgevoerde onderzoek, kunt u zich zowel nu als in de toekomst uiteraard tot mij wenden.

Het zou fantastisch zijn als dit eenmalige interview plaats zou kunnen vinden in de week van 10 t/m 14 februari. Naar verwachting is een uur voldoende.

Met vriendelijke groet

Noury Takens

Appendix 4: Plan for analysis of the results

Plan for analysis of the results – Before going into analysis, we will first increase the quality of the collected data. In their article, Meade & Craig (2012) are giving several recommendations on how to do this, and we are applying their method with regards to non-responsivity. This means that we identify and exclude the results where respondents have selected e.g. 'disagree' to every statement.

After this step has been taken, we are setting up a score structure for the level of ISA. Here, we are following the approach of Pattinson et al. (2016). This will be the starting point of our analysis and will provide a general view on the scores of the two groups. The reverse scoring items will be transformed to fit with the total set of questions. We are presenting the ISA scores in the form of percentages and to do this, we will take the 'agree' and strongly agree' answers and divide them by the total number of responses given by the respondent. Based on these scores, we will firstly present one matrix of scores on the KAB dimensions, focus areas and total ISA, showing the results of all the headquarters and branch employees. Secondly, we will apply the Mann-Whitney U test within our set of data. When it adds value, visualization of the results will be applied by using tables, pie charts and/or bar charts. The presentation of the results will be as follows:

- **Differences on general ISA between both user groups**
- **Differences on the user groups' awareness within the focus areas**

After doing a thorough analysis of the data, we are able to draw conclusions and provide recommendations for further research.

Appendix 5: Setup & settings R-HAIS-Q

Text elements	
Survey title:	Information Security Awareness amongst banking employees
Base language	English
Description	-
Welcome message	Dear colleague, As part of my Master thesis, I am doing a research project on Information Security Awareness amongst banking employees. It is **highly appreciated** if you could take part in this survey, which will take about 8 minutes of your time to complete. Your participation is entirely voluntary and your responses will be treated strictly confidential. If you have any questions, please do not hesitate to contact me at noury.takens@rabobank.nl. Thank you. Noury Takens
End message:	Thank you for taking the time to complete this survey. Kindest regards, Noury Takens
Create example question group and question?	No
General settings	
Survey owner	852061695 - Noury Takens
Administrator	Noury Takens
Admin email	isa-questionnaire@ou.nl
Bounce email	isa-questionnaire@ou.nl
Fax to	-
Group	Default
Format	Group by group
Template	fruity_OU
Presentation & navigation	
Navigation delay (seconds)	0
Show question index / allow jumping	Disabled
Show group name and/or group description	Show both
Show question number and/or code	Hide both
Show "no answer"	On (forced by system administrator)
Show "there are X questions in this survey	Off
Show welcome screen	On
Allow backward navigation	Off
Show on-screen keyboard	Off
Show progress bar	On
Participants may print answers	Off
Public statistics	Off
Show graphs in public statistics	Off
Automatically load URL when survey complete	Off
Publication and access control	
Start date/time	07-04-2020
Expiry date/time	22-04-2020
List survey publicly	Off
Set cookie to prevent repeated participation	Off
Use CAPTCHA for survey access	Off
Use CAPTCHA for registration	Off
Use CAPTCHA for save and load	Off
Notification and data management	
Date stamp	Off
Save IP address	Off
Save referrer URL	Off
Save timings	Off
Enable assessment mode	Off
Participant may save and resume later	On
Send basic admin notification email to	isa-questionnaire@ou.nl
Send detailed admin notification email to	isa-questionnaire@ou.nl
Google analytics settings	Off
Participant settings	
Set token length to	15
Anonymized responses	On
Enable token-based response persistence	Off
Allow multiple responses or update responses with one token	Off
Allow public registration	Off
Use HTML format for token emails	On
Send confirmation emails	On

Appendix 6: R-HAIS-Q

Group:	**General information**					
Introduction:	First, you will be asked to provide answers to several general questions.					
Code	**Definition**	**Question**			**Question type**	**Answer possibilities**
GEN1	Gender of respondent	What is your gender?			Gender	Male / Female / No answer
AGE1	Age of respondent	What is your age?			List (radio)	18-25 years old / 26-40 years old / 41-55 years old / 56-68 years old / 69 or older / No answer
EDU1	Educational level	What is the level of school you have completed?			List (radio)	Secondary vocational education (MBO) / Higher professional education (HBO) / University education (WO) / No answer
LOC1	Working location	Where do you work?			List (radio)	Head office / Local bank / No answer
CCO1	Client contact	To what extent do you have contact with clients? Help text: *With clients, we mean external clients (e.g. clients having bank accounts, loans etc.)*			List (radio)	Yes, I do have contact with clients on a daily basis / No, I never have contact with clients / No answer
Group:	**Knowledge of computer use guidelines**					
Introduction:	You will now be asked to complete three sets of questions about how you manage your passwords. These sets of questions are about: - Your knowledge of password management guidelines; - Your attitude towards these guidelines; - Your behaviour regarding managing your passwords.					
Description:	The following statements are about your knowledge of how you should use a computer for work. *Please note: statements regarding social media are related to your personal social media accounts (not e.g. Yammer).*					
Code	**Focus area**	**Question**			**Question type**	**Answer possibilities**	**Reverse scoring?**
KNM10	Mobile devices	When working in a public place, I have to keep my laptop with me at all times.			Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	N
KNE04	Email use	I am allowed to click on any links in emails from people I know.			Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	Y
KNS07	Social media use	I must periodically review the privacy settings on my social media accounts.			Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	N
KNP01	Password management	It's acceptable to use my social media passwords on my work accounts.			Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	Y
KNI13	Incident reporting	If I see someone acting suspiciously in my workplace, I should report it.			Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	N
KNE06	Email use	I am allowed to open email attachments from unknown senders.			Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	Y
KNS09	Social media use	I can post what I want about work on social media.			Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	Y
KNI15	Incident reporting	It's optional to report security incidents.			Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	Y
KNM12	Mobile devices	When working on a sensitive document, I must ensure that strangers can't see my laptop screen.			Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	N
KNP03	Password management	A mixture of letters, numbers and symbols is necessary for my work passwords.			Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	N
KNE05	Email use	I am not permitted to click on a link in an email from an unknown sender.			Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	N
KNP02	Password management	I am allowed to share my work passwords with my colleagues.			Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	Y
KNM11	Mobile devices	I am allowed to send work files via a public Wi-Fi network.			Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	Y
KNI14	Incident reporting	I must not ignore poor security behavior by my colleagues.			Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	N
KNS08	Social media use	I can't be fired for something I post on social media.			Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	Y

Group:	Attitude towards computer use guidelines				
Introduction:	-				
Description:	The following statements are about your attitude. You've told us about your knowledge of computer use guidelines. Now please tell us what you think about these guidelines. *Please note: statements regarding social media are related to your personal social media accounts (not e.g. Yammer).*				
Code	**Focus area**	**Question**	**Question type**	**Answer possibilities**	**Reverse scoring?**
ATP02	Password management	It's a bad idea to share my work passwords, even if a colleague asks for it.	Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	N
ATE05	Email use	Nothing bad can happen if I click on a link in an email from an unknown sender.	Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	Y
ATP01	Password management	It's safe to use the same password for social media and work accounts.	Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	Y
ATS09	Social media use	It's risky to post certain information about my work on social media.	Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	N
ATM12	Mobile devices	It's risky to to access sensitive work files on a laptop if strangers can see my screen.	Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	N
ATS08	Social media use	It doesn't matter if I post things on social media that I wouldn't normally say in public.	Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	Y
ATE06	Email use	It's risky to open an email attachment from an unknown sender.	Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	N
ATI14	Incident reporting	Nothing bad can happen if I ignore poor security behavior by a colleague.	Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	Y
ATE04	Email use	It's always safe to click on links in emails from people I know.	Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	Y
ATI15	Incident reporting	It's risky to ignore security incidents, even if I think they're not significant.	Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	N
ATP03	Password management	It's safe to have a work password with just letters	Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	Y
ATS07	Social media use	It's a good idea to regularly review my social media privacy settings.	Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	N
ATM10	Mobile devices	When working in a café, it's safe to leave my laptop unattended for a minute.	Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	Y
ATI13	Incident reporting	If I ignore someone acting suspiciously in my workplace, nothing bad can happen.	Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	Y
ATM11	Mobile devices	It's risky to send sensitive work files using a public Wi-Fi network.	Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	N
Group:	**Behavior when using a computer for work**				
Introduction:	-				
Description:	The following statements are about your behavior. You've told us what you know, and what you think about computer use guidelines. Now please tell us what you do when using a computer for work. *Please note: statements regarding social media are related to your personal social media accounts (not e.g. Yammer).*				
Code	**Focus area**	**Question**	**Question type**	**Answer possibilities**	**Reverse scoring?**
BEE05	Email use	If an email from an unknown sender looks interesting, I click on a link within it.	Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	Y
BES09	Social media use	I post whatever I want about my work on social media.	Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	Y
BEP01	Password management	I use a different password for my social media and work accounts.	Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	N
BEI15	Incident reporting	If I noticed a security incident, I would report it.	Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	N
BEP03	Password management	I use a combination of letters, numbers and symbols in my work passwords.	Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	N
BES07	Social media use	I don't regularly review my social media privacy settings.	Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	Y
BEM10	Mobile devices	When working in a public place, I leave my laptop unattended.	Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	Y
BEE06	Email use	I don't open email attachments if the sender is unknown to me.	Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	N
BEM11	Mobile devices	I send sensitive work files using a public Wi-Fi network.	Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	Y
BEI13	Incident reporting	If I saw someone acting suspiciously in my workplace, I would do something about it.	Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	N
BEP02	Password management	I share my work passwords with colleagues.	Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	Y
BES08	Social media use	I don't post anything on social media before considering any negative consequences.	Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	N
BEM12	Mobile devices	I check that strangers can't see my laptop screen if I'm working on a sensitive document.	Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	N
BEI14	Incident reporting	If I noticed my colleague ignoring security rules, I wouldn't take any action.	Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	Y
BEE04	Email use	I don't always click on links in emails just because they come from someone I know.	Array	Strongly disagree - Disagree - Undecided - Agree - Strongly agree - Not applicable	N

Appendix 7: R-HAIS-Q results

HEADQUARTER EMPLOYEE RESULTS - REVERSE SCORING APPLIED

Knowledge

					Low ISA				*High ISA*			
					1	**2**	**3**	**4**	**5**			
Code	**Focus area**	**Question**	**Reverse scoring?**		**Strongly disagree**	**Disagree**	**Undecided**	**Agree**	**Strongly agree**	**Not applicable**	**Respondents**	**%**
KNP01	Password management	It's acceptable to use my social media passwords on my work accounts.	Y		0	1	0	13	17	0	31	96,77
KNP02	Password management	I am allowed to share my work passwords with my colleagues.	Y		0	0	1	3	27	0	31	96,77
KNP03	Password management	A mixture of letters, numbers and symbols is necessary for my work passwords.	N		0	1	0	14	16	0	31	96,77
KNE04	Email use	I am allowed to click on any links in emails from people I know.	Y		0	2	3	16	10	0	31	83,87
KNE05	Email use	I am not permitted to click on a link in an email from an unknown sender.	N		2	3	5	7	14	0	31	67,74
KNE06	Email use	I am allowed to open email attachments from unknown senders.	Y		1	2	2	5	21	0	31	83,87
KNS07	Social media use	I must periodically review the privacy settings on my social media accounts.	N		0	1	5	14	7	4	31	77,78
KNS08	Social media use	I can't be fired for something I post on social media.	Y		1	2	0	16	12	0	31	90,32
KNS09	Social media use	I can post what I want about work on social media.	Y		1	0	0	9	21	0	31	96,77
KNM10	Mobile devices	When working in a public place, I have to keep my laptop with me at all times.	N		1	0	1	2	26	1	31	93,33
KNM11	Mobile devices	I am allowed to send work files via a public Wi-Fi network.	Y		0	1	3	10	17	0	31	87,10
KNM12	Mobile devices	When working on a sensitive document, I must ensure that strangers can't see my lap	N		0	0	0	5	26	0	31	100,00
KNI13	Incident reporting	If I see someone acting suspiciously in my workplace, I should report it.	N		0	0	1	13	17	0	31	96,77
KNI14	Incident reporting	I must not ignore poor security behavior by my colleagues.	N		0	2	1	13	15	0	31	90,32
KNI15	Incident reporting	It's optional to report security incidents.	Y		0	2	1	10	18	0	31	90,32

Attitude

					Low ISA				*High ISA*			
					1	**2**	**3**	**4**	**5**			
Code	**Focus area**	**Question**	**Reverse scoring?**		**Strongly disagree**	**Disagree**	**Undecided**	**Agree**	**Strongly agree**	**Not applicable**	**Respondents**	**%**
ATP01	Password management	It's safe to use the same password for social media and work accounts.	Y		0	1	0	12	18	0	31	96,77
ATP02	Password management	It's a bad idea to share my work passwords, even if a colleague asks for it.	N		0	0	1	3	27	0	31	96,77
ATP03	Password management	It's safe to have a work password with just letters	Y		0	1	0	16	14	0	31	96,77
ATE04	Email use	It's always safe to click on links in emails from people I know.	Y		0	0	2	16	13	0	31	93,55
ATE05	Email use	Nothing bad can happen if I click on a link in an email from an unknown sender.	Y		0	0	0	7	24	0	31	100,00
ATE06	Email use	It's risky to open an email attachment from an unknown sender.	N		0	1	1	9	20	0	31	93,55
ATS07	Social media use	It's a good idea to regularly review my social media privacy settings.	N		0	0	1	18	9	3	31	96,43
ATS08	Social media use	It doesn't matter if I post things on social media that I wouldn't normally say in public.	Y		0	2	0	12	17	0	31	93,55
ATS09	Social media use	It's risky to post certain information about my work on social media.	N		0	0	1	18	12	0	31	96,77
ATM10	Mobile devices	When working in a café, it's safe to leave my laptop unattended for a minute.	Y		1	0	0	4	26	0	31	96,77
ATM11	Mobile devices	It's risky to send sensitive work files using a public Wi-Fi network.	N		1	1	1	8	20	0	31	90,32
ATM12	Mobile devices	It's risky to to access sensitive work files on a laptop if strangers can see my screen.	N		0	0	0	9	22	0	31	100,00
ATI13	Incident reporting	If I ignore someone acting suspiciously in my workplace, nothing bad can happen.	Y		0	0	1	14	16	0	31	96,77
ATI14	Incident reporting	Nothing bad can happen if I ignore poor security behavior by a colleague.	Y		0	1	0	16	14	0	31	96,77
ATI15	Incident reporting	It's risky to ignore security incidents, even if I think they're not significant.	N		0	0	1	13	17	0	31	96,77

Behavior												
					Low ISA				*High ISA*			
					1	**2**	**3**	**4**	**5**			
Code	**Focus area**	**Question**	**Reverse scoring?**		**Strongly disagree**	**Disagree**	**Undecided**	**Agree**	**Strongly agree**	**Not applicable**	**Respondents**	**%**
BEP01	Password management	I use a different password for my social media and work accounts.	N		1	2	1	11	15	1	31	86,67
BEP02	Password management	I share my work passwords with colleagues.	Y		0	0	0	9	22	0	31	100,00
BEP03	Password management	I use a combination of letters, numbers and symbols in my work passwords.	N		0	1	1	11	18	0	31	93,55
BEE04	Email use	I don't always click on links in emails just because they come from someone I know.	N		2	2	3	15	9	0	31	77,42
BEE05	Email use	If an email from an unknown sender looks interesting, I click on a link within it.	Y		0	0	0	13	18	0	31	100,00
BEE06	Email use	I don't open email attachments if the sender is unknown to me.	N		1	0	3	9	18	0	31	87,10
BES07	Social media use	I don't regularly review my social media privacy settings.	Y		0	8	1	14	5	3	31	67,86
BES08	Social media use	I don't post anything on social media before considering any negative consequences.	N		0	0	0	8	20	3	31	100,00
BES09	Social media use	I post whatever I want about my work on social media.	Y		2	0	0	9	19	1	31	93,33
BEM10	Mobile devices	When working in a public place, I leave my laptop unattended.	Y		0	0	2	5	24	0	31	93,55
BEM11	Mobile devices	I send sensitive work files using a public Wi-Fi network.	Y		0	2	0	8	21	0	31	93,55
BEM12	Mobile devices	I check that strangers can't see my laptop screen if I'm working on a sensitive docume	N		0	0	2	9	19	1	31	93,33
BEI13	Incident reporting	If I saw someone acting suspiciously in my workplace, I would do something about it.	N		0	1	2	16	12	0	31	90,32
BEI14	Incident reporting	If I noticed my colleague ignoring security rules, I wouldn't take any action.	Y		1	4	2	13	11	0	31	77,42
BEI15	Incident reporting	If I noticed a security incident, I would report it.	N		0	1	2	16	12	0	31	90,32

BRANCH EMPLOYEE RESULTS - REVERSE SCORING APPLIED

Knowledge												
					Low ISA				*High ISA*			
					1	**2**	**3**	**4**	**5**			
Code	**Focus area**	**Question**	**Reverse scoring?**		**Strongly disagree**	**Disagree**	**Undecided**	**Agree**	**Strongly agree**	**Not applicable**	**Respondents**	**%**
KNP01	Password management	It's acceptable to use my social media passwords on my work accounts.	Y		0	4	2	16	11	1	34	81,82
KNP02	Password management	I am allowed to share my work passwords with my colleagues.	Y		1	0	1	7	25	0	34	94,12
KNP03	Password management	A mixture of letters, numbers and symbols is necessary for my work passwords.	N		0	0	3	13	17	1	34	90,91
KNE04	Email use	I am allowed to click on any links in emails from people I know.	Y		0	3	2	23	6	0	34	85,29
KNE05	Email use	I am not permitted to click on a link in an email from an unknown sender.	N		0	2	2	15	15	0	34	88,24
KNE06	Email use	I am allowed to open email attachments from unknown senders.	Y		0	0	0	14	20	0	34	100,00
KNS07	Social media use	I must periodically review the privacy settings on my social media accounts.	N		1	4	6	19	3	1	34	66,67
KNS08	Social media use	I can't be fired for something I post on social media.	Y		1	6	10	11	6	0	34	50,00
KNS09	Social media use	I can post what I want about work on social media.	Y		1	0	1	5	27	0	34	94,12
KNM10	Mobile devices	When working in a public place, I have to keep my laptop with me at all times.	N		0	1	0	3	30	0	34	97,06
KNM11	Mobile devices	I am allowed to send work files via a public Wi-Fi network.	Y		3	0	4	13	14	0	34	79,41
KNM12	Mobile devices	When working on a sensitive document, I must ensure that strangers can't see my lap	N		1	0	0	9	24	0	34	97,06
KNI13	Incident reporting	If I see someone acting suspiciously in my workplace, I should report it.	N		0	0	3	17	14	0	34	91,18
KNI14	Incident reporting	I must not ignore poor security behavior by my colleagues.	N		3	1	3	16	11	0	34	79,41
KNI15	Incident reporting	It's optional to report security incidents.	Y		1	6	1	11	15	0	34	76,47

Attitude

					Low ISA				*High ISA*			
					1	**2**	**3**	**4**	**5**			
Code	**Focus area**	**Question**	**Reverse scoring?**		**Strongly disagree**	**Disagree**	**Undecided**	**Agree**	**Strongly agree**	**Not applicable**	**Respondents**	**%**
ATP01	Password management	It's safe to use the same password for social media and work accounts.	Y		0	2	1	18	13	0	34	91,18
ATP02	Password management	It's a bad idea to share my work passwords, even if a colleague asks for it.	N		0	0	1	6	27	0	34	97,06
ATP03	Password management	It's safe to have a work password with just letters	Y		1	1	6	17	9	0	34	76,47
ATE04	Email use	It's always safe to click on links in emails from people I know.	Y		0	0	1	24	9	0	34	97,06
ATE05	Email use	Nothing bad can happen if I click on a link in an email from an unknown sender.	Y		0	0	0	16	18	0	34	100,00
ATE06	Email use	It's risky to open an email attachment from an unknown sender.	N		0	1	1	12	20	0	34	94,12
ATS07	Social media use	It's a good idea to regularly review my social media privacy settings.	N		1	1	6	23	3	0	34	76,47
ATS08	Social media use	It doesn't matter if I post things on social media that I wouldn't normally say in public	Y		1	0	2	12	19	0	34	91,18
ATS09	Social media use	It's risky to post certain information about my work on social media.	N		0	0	1	22	11	0	34	97,06
ATM10	Mobile devices	When working in a café, it's safe to leave my laptop unattended for a minute.	Y		2	0	0	6	26	0	34	94,12
ATM11	Mobile devices	It's risky to send sensitive work files using a public Wi-Fi network.	N		0	0	1	14	19	0	34	97,06
ATM12	Mobile devices	It's risky to to access sensitive work files on a laptop if strangers can see my screen.	N		0	0	0	14	20	0	34	100,00
ATI13	Incident reporting	If I ignore someone acting suspiciously in my workplace, nothing bad can happen.	Y		0	0	1	18	15	0	34	97,06
ATI14	Incident reporting	Nothing bad can happen if I ignore poor security behavior by a colleague.	Y		0	0	0	23	11	0	34	100,00
ATI15	Incident reporting	It's risky to ignore security incidents, even if I think they're not significant.	N		1	1	3	19	10	0	34	85,29

Behavior

					Low ISA				*High ISA*			
					1	**2**	**3**	**4**	**5**			
Code	**Focus area**	**Question**	**Reverse scoring?**		**Strongly disagree**	**Disagree**	**Undecided**	**Agree**	**Strongly agree**	**Not applicable**	**Respondents**	**%**
BEP01	Password management	I use a different password for my social media and work accounts.	N		1	2	0	16	15	0	34	91,18
BEP02	Password management	I share my work passwords with colleagues.	Y		0	1	2	6	25	0	34	91,18
BEP03	Password management	I use a combination of letters, numbers and symbols in my work passwords.	N		0	5	2	14	13	0	34	79,41
BEE04	Email use	I don't always click on links in emails just because they come from someone I know.	N		0	4	4	19	7	0	34	76,47
BEE05	Email use	If an email from an unknown sender looks interesting, I click on a link within it.	Y		0	1	4	15	14	0	34	85,29
BEE06	Email use	I don't open email attachments if the sender is unknown to me.	N		0	2	3	17	12	0	34	85,29
BES07	Social media use	I don't regularly review my social media privacy settings.	Y		1	13	6	11	2	1	34	39,39
BES08	Social media use	I don't post anything on social media before considering any negative consequences.	N		0	0	1	17	16	0	34	97,06
BES09	Social media use	I post whatever I want about my work on social media.	Y		0	0	1	19	14	0	34	97,06
BEM10	Mobile devices	When working in a public place, I leave my laptop unattended.	Y		0	0	1	8	24	1	34	96,97
BEM11	Mobile devices	I send sensitive work files using a public Wi-Fi network.	Y		1	1	1	20	11	0	34	91,18
BEM12	Mobile devices	I check that strangers can't see my laptop screen if I'm working on a sensitive docume	N		0	1	1	14	17	1	34	93,94
BEI13	Incident reporting	If I saw someone acting suspiciously in my workplace, I would do something about it.	N		0	0	1	23	10	0	34	97,06
BEI14	Incident reporting	If I noticed my colleague ignoring security rules, I wouldn't take any action.	Y		0	3	4	19	8	0	34	79,41
BEI15	Incident reporting	If I noticed a security incident, I would report it.	N		0	0	3	18	13	0	34	91,18

Appendix 8: Mann Whitney U test statistics

Mann Whitney U test - Password Management

					Headquarter employees			Branch employees			Test statistics			
Nr.	Code:	KAB dimension	Sub-area	Statement	N	Mean Rank	Sum of Ranks	N	Mean Rank	Sum of Ranks	Mann Whitney U	Wilcoxon W	Z	Asymp. Sig. (2-tailed)
1	KNP01	Knowledge	Using the same password	It's acceptable to use my social media passwords on my work accounts.	31	34.97	1084.00	33	30.18	996.00	435.000	996.000	-1901	.057
2	ATP01	Attitude	Using the same password	It's safe to use the same password for social media and work accounts.	31	33.95	1052.50	34	32.13	1092.50	497.500	1092.500	-.931	.352
3	BEP01	Behavior	Using the same password	I use a different password for my social media and work accounts.	30	31.73	952.00	34	33.18	1128.00	487.000	952.000	-.572	.567
4	KNP02	Knowledge	Sharing passwords	I am allowed to share my work passwords with my colleagues.	31	33.45	1037.00	34	32.59	1108.00	513.000	1108.000	-.506	.613
5	ATP02	Attitude	Sharing passwords	It's a bad idea to share my work passwords, even if a colleague asks for it.	31	31.95	1021.50	34	33.04	1123.50	525.500	1021.500	-.066	.947
6	BEP02	Behavior	Sharing passwords	I share my work passwords with colleagues.	31	34.50	1069.50	34	31.63	1075.50	480.500	1075.500	-1.680	.093
7	KNP03	Knowledge	Using a strong password	A mixture of letters, numbers and symbols is necessary for my work passwords.	31	33.47	1037.50	33	31.59	1042.50	481.500	1042.500	-.961	.336
8	ATP03	Attitude	Using a strong password	It's safe to have a work password with just letters	31	36.45	1130.00	34	29.85	1015.00	420.000	1015.000	-2.349	.019
9	BEP03	Behavior	Using a strong password	I use a combination of letters, numbers and symbols in my work passwords.	31	35.40	1097.50	34	30.81	1047.50	452.500	1047.500	-1.635	.102

Mann Whitney U test - Email Use

					Headquarter employees			Branch employees			Test statistics			
Nr.	Code:	KAB dimension	Sub-area	Statement	N	Mean Rank	Sum of Ranks	N	Mean Rank	Sum of Ranks	Mann Whitney U	Wilcoxon W	Z	Asymp. Sig. (2-tailed)
1	KNE04	Knowledge	Clicking on links in emails (known senders)	I am allowed to click on any links in emails from people I know.	31	32.76	1015.50	34	33.22	1129.50	519.500	1015.500	-.158	.875
2	ATE04	Attitude	Clicking on links in emails (known senders)	It's always safe to click on links in emails from people I know.	31	32.40	1004.50	34	33.54	1140.50	508.500	1004.500	-.669	.504
3	BEE04	Behavior	Clicking on links in emails (known senders)	I don't always click on links in emails just because they come from someone I know.	31	33.16	1028.00	34	32.85	1117.00	522.000	1117.000	-.090	.928
4	KNE05	Knowledge	Clicking on links in emails (unknown senders)	I am not permitted to click on a link in an email from an unknown sender.	31	29.52	915.00	34	36.18	1230.00	419.000	915.000	-1.992	.046
5	ATE05	Attitude	Clicking on links in emails (unknown senders)	Nothing bad can happen if I click on a link in an email from an unknown sender.	31	33.00	1023.00	34	33.00	1122.00	527.000	1122.000	.000	1.000
6	BEE05	Behavior	Clicking on links in emails (unknown senders)	If an email from an unknown sender looks interesting, I click on a link within it.	31	35.50	1100.50	34	30.72	1044.50	449.500	1044.500	-2.205	.027
7	KNE06	Knowledge	Opening attachments in emails (unk. senders)	I am allowed to open email attachments from unknown senders.	31	30.26	938.00	34	35.50	1207.00	442.000	938.000	-2.419	.016
8	ATE06	Attitude	Opening attachments in emails (unk. senders)	It's risky to open an email attachment from an unknown sender.	31	32.90	1020.00	34	33.09	1125.00	524.000	1020.000	-.095	.925
9	BEE06	Behavior	Opening attachments in emails (unk. senders)	I don't open email attachments if the sender is unknown to me.	31	33.31	1032.50	34	32.72	1112.50	517.500	1112.500	-.209	.835

Mann Whitney U test - Social Media Use

					Headquarter employees			Branch employees			Test statistics			
Nr.	Code:	KAB dimension	Sub-area	Statement	N	Mean Rank	Sum of Ranks	N	Mean Rank	Sum of Ranks	Mann Whitney U	Wilcoxon W	Z	Asymp. Sig. (2-tailed)
1	KNS07	Knowledge	SM privacy settings	I must periodically review the privacy settings on my social media accounts.	27	32.33	873.00	33	29.00	957.00	396.000	957.000	-.942	.346
2	ATS07	Attitude	SM privacy settings	It's a good idea to regularly review my social media privacy settings.	28	34.89	977.00	34	28.71	976.00	381.000	976.000	-2.202	.028
3	BES07	Behavior	SM privacy settings	I don't regularly review my social media privacy settings.	28	35.70	999.50	33	27.02	891.50	330.500	891.500	-2.200	.028
4	KNS08	Knowledge	Considering consequences	I can't be fired for something I post on social media.	31	39.85	1235.50	34	26.75	909.50	314.500	909.500	-3.491	.000
5	ATS08	Attitude	Considering consequences	It doesn't matter if I post things on social media that I wouldn't normally say in public.	31	33.40	1035.50	34	32.63	1109.50	514.500	1109.500	-.356	.722
6	BES08	Behavior	Considering consequences	I don't post anything on social media before considering any negative consequences.	28	32.00	896.00	34	31.09	1057.00	462.000	1057.000	-.907	.364
7	KNS09	Knowledge	Posting about work	I can post what I want about work on social media.	31	33.45	1037.00	34	32.59	1108.00	513.000	1108.000	-.506	.613
8	ATS09	Attitude	Posting about work	It's risky to post certain information about my work on social media.	31	32.95	1021.50	34	33.04	1023.50	525.500	1021.500	-.066	.947
9	BES09	Behavior	Posting about work	I post whatever I want about my work on social media.	30	31.87	956.00	34	33.06	1124.00	491.000	956.000	-.698	.485

Mann Whitney U test - Mobile Devices

					Headquarter employees			Branch employees			Test statistics			
Nr.	Code:	KAB dimension	Sub-area	Statement	N	Mean Rank	Sum of Ranks	N	Mean Rank	Sum of Ranks	Mann Whitney U	Wilcoxon W	Z	Asymp. Sig. (2-tailed)
1	KNM10	Knowledge	Physically securing mobile devices	When working in a public place, I have to keep my laptop with me at all times.	30	31.87	956.00	34	33.06	1124.00	491.000	956.000	-.698	.485
2	ATM10	Attitude	Physically securing mobile devices	When working in a café, it's safe to leave my laptop unattended for a minute.	31	33.45	1037.00	34	32.59	1108.00	513.000	1108.000	-.506	.613
3	BEM10	Behavior	Physically securing mobile devices	When working in a public place, I leave my laptop unattended.	31	31.94	990.00	33	33.03	1090.00	494.000	990.000	-.642	.521
4	KNM11	Knowledge	Sending sensitive information via Wi-Fi	I am allowed to send work files via a public Wi-Fi network.	31	34.31	1063.50	34	31.81	1081.50	486.500	1081.500	-.819	.413
5	ATM11	Attitude	Sending sensitive information via Wi-Fi	It's risky to send sensitive work files using a public Wi-Fi network.	31	31.85	987.50	34	34.04	1157.50	491.500	987.500	-1.120	.263
6	BEM11	Behavior	Sending sensitive information via Wi-Fi	I send sensitive work files using a public Wi-Fi network.	31	33.40	1035.50	34	32.63	1109.50	514.500	1109.500	-.356	.722
7	KNM12	Knowledge	Shoulder surfing	When working on a sensitive document, I must ensure that strangers can't see my lap	31	33.50	1038.50	34	32.54	1106.50	511.500	1106.500	-.955	.340
8	ATM12	Attitude	Shoulder surfing	It's risky to to access sensitive work files on a laptop if strangers can see my screen.	31	33.00	1023.00	34	33.00	1122.00	527.000	1122.000	.000	1.000
9	BEM12	Behavior	Shoulder surfing	I check that strangers can't see my laptop screen if I'm working on a sensitive docume	30	31.90	957.00	33	32.09	1059.00	492.000	957.000	-.098	.922

Mann Whitney U test - Incident Reporting

					Headquarter employees			Branch employees			Test statistics			
Nr.	Code:	KAB dimension	Sub-area	Statement	N	Mean Rank	Sum of Ranks	N	Mean Rank	Sum of Ranks	Mann Whitney U	Wilcoxon W	Z	Asymp. Sig. (2-tailed)
1	KNI13	Knowledge	Reporting suspicious behavior	If I see someone acting suspiciously in my workplace, I should report it.	31	33.95	1052.50	34	32.13	1092.50	497.500	1092.500	-.931	.352
2	ATI13	Attitude	Reporting suspicious behavior	If I ignore someone acting suspiciously in my workplace, nothing bad can happen.	31	32.95	1021.50	34	33.04	1123.50	525.500	1021.500	-.066	.947
3	BEI13	Behavior	Reporting suspicious behavior	If I saw someone acting suspiciously in my workplace, I would do something about it.	31	31.85	987.50	34	34.04	1157.50	491.500	987.500	-1.120	.263
4	KNI14	Knowledge	Ignoring poor security behavior by colleagues	I must not ignore poor security behavior by my colleagues.	31	34.85	1080.50	34	31.31	1064.50	469.500	1064.500	-1.208	.227
5	ATI14	Attitude	Ignoring poor security behavior by colleagues	Nothing bad can happen if I ignore poor security behavior by a colleague.	31	32.45	1006.00	34	33.50	1139.00	510.000	1006.000	-1.047	.295
6	BEI14	Behavior	Ignoring poor security behavior by colleagues	If I noticed my colleague ignoring security rules, I wouldn't take any action.	31	32.66	1012.50	34	33.31	1132.50	516.500	1012.500	-.194	.846
7	KNI15	Knowledge	Reporting all incidents	It's optional to report security incidents.	31	35.35	1096.00	34	30.85	1049.00	454.000	1049.000	-1.476	.140
8	ATI15	Attitude	Reporting all incidents	It's risky to ignore security incidents, even if I think they're not significant.	31	34.95	1083.50	34	31.22	1061.50	466.500	1061.500	-1.585	.113
9	BEI15	Behavior	Reporting all incidents	If I noticed a security incident, I would report it.	31	32.85	1018.50	34	33.13	1126.50	522.500	1018.500	-.118	.906